UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

André Bereza Júnior

AUDITORIA UNIFICADA EM MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA

Florianópolis

2013

André Bereza Júnior

AUDITORIA UNIFICADA EM MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA

Dissertação submetida ao Programa de Pós-Graduação em Ciência da Computação para a obtenção do Grau de mestre em Ciência da Computação.

Prof. Ricardo Felipe Custódio, Dr.
Orientador

Florianópolis

2013

Catalogação na fonte elaborada pela biblioteca da
Universidade Federal de Santa Catarina

A ficha catalográfica é confeccionada pela Biblioteca Central.

Tamanho: 7cm x 12 cm

Fonte: Times New Roman 9,5

Maiores informações em:
http://www.bu.ufsc.br/design/Catalogacao.html

André Bereza Júnior

AUDITORIA UNIFICADA EM MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA

Esta Dissertação foi julgada aprovada para a obtenção do título de mestre em Ciência da Computação, e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Florianópolis, 05 de Fevereiro 2013

Prof. Ronaldo dos Santos Mello, Dr.
Coordenador do Curso

Banca Examinadora:

Prof. Ricardo Felipe Custódio, Dr.
Orientador
Universidade Federal de Santa Catarina

Prof. Ricardo Dahab, Dr.
Universidade Estadual de Campinas

Prof. Ricardo Alexandre Reinaldo de Moraes, Dr.
Universidade Federal de Santa Catarina

Profa. Michelle Silva Wangham, Dr.
Universidade do Vale do Itajaí

RESUMO

Este trabalho tem como objetivo tornar a detecção da causa de ataques em HSMs uma informação de conhecimento dos proprietários de um dispositivo, sem que essa informação seja perdida. A auditoria e detecção de como um ataque ocorreu em um HSM não pode ser algo que se perde durante o ciclo de vida de um HSM.
A proposta deste trabalho é unificar a auditoria de HSMs, para que um ataque que ocorreu no dispositivo possa ser detectado em qualquer momento do seu ciclo de vida. É necessário que o proprietário do HSM saiba que ataque ocorreu, quando ocorreu e quem executou o ataque.
Para atingir este objetivo foi realizada a leitura do ciclo de vida de um HSM, apresentando as suas etapas. A partir de cada etapa do ciclo de vida é possível gerar rastros de auditoria, que podem ser utilizados a qualquer momento em um processo de auditoria.
Para que os rastros de auditoria sejam gerados em HSMs e para que a auditoria unificada seja um padrão entre dispositivos, é necessário adequar as normas de homologação e padronização de HSMs para garantir a interoperabilidade entre os dispositivos. Este trabalho apresenta formas de se adequar as normas FIPS 140-2 e MCT 7 para que HSMs homologados sob essas normas possuam funcionalidades capazes de gerar rastros de auditoria.

Palavras-chave: HSM, Módulo de Segurança Criptográfica, Auditoria

ABSTRACT

The objective of this work is to make the cause of attacks an information that the HSM's owners will have access, without losing this information. The audit and detection of how an attack occurred in an HSM cannot lose itself during an HSM life-cycle.
This work proposal is to unify the HSM audit, so that an attack that happened in the device can be detected in any moment of its life-cycle. The HSM owner needs to know that the attack happened, when it happened and who executed it.
To achieve this objetive, the HSM life-cycle is presented with its stages. From every life-cycle stage it is possible to generate audit traces, that can be used at any momento in an audit process.
To make sure that the audit traces are generated in HSMs and that the unified audit is an standard in those devices, it is necessary to adapt the evaluation standards to guarantee the interoperability between those devices. This work presents ways of adapting the FIPS 140-2 and MCT 7 standards, so that the HSMs that are evaluated by these standards have functions that allow them to generate audit traces.

Keywords: HSM, Hardware Security Module, Audit

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

SUMÁRIO

1 INTRODUÇÃO

Sistemas de informação e comunicação, em geral, utilizam algoritmos criptográficos para a proteção de dados. Esses algoritmos são usados não somente para o sigilo da informação, mas também para garantir a integridade e autenticidade desses sistemas e de seus dados.

É sabido que algoritmos criptográficos utilizam senhas, ou mais especificamente, sequencias de códigos binários - conhecidos como chaves criptográficas - como parâmetros no processo de cifragem e decifragem dos dados.

Essas chaves precisam ser geradas e mantidas fora do alcance de entidades não autorizadas. No entanto, para que um sistema de informação execute um algoritmo criptográfico, este precisa de acesso a chave, E esse acesso pode ser indevidamente monitorado por um atacante para utilizar a chaves sem autorizaçãoou até para realizar a cópia da chave e posteriormente decifrar dados sigilosos.

Uma forma bastante interessante de proteger as chaves chaves criptográficas é através do uso de dispositivos eletrônicos especialmente concebidos para essa tarefa. Dentre esses dispositivos estão o smartcard e os módulos de segurança criptográfica.

Tanto os smartcards quantos os módulos de segurança criptográfica permitem o uso da chave sem revelar a mesma ao sistema. Eles operam da seguinte forma: a) o sistema se autentica no dispositivo criptografico; b) após o sucesso da autenticação, a mensagem a ser cifrada é enviada ao dispositivo; c) o dispositivo cifra a mensagem, internamente; d) a mensagem cifrada é enviada pelo dispositivo para o sistema. Dessa forma a chave nunca é disponibilizada ou mesmo revelada ao sistema, e portanto, mesmo que o sistema esteja sendo monitorado, a chave não pode ser utilizada.

Smartcards são mais adequados a proteção de chaves criptográficas de pessoas, pois permitem que seu dono a leve consigo. Ou seja, permitem a mobilidade. A ideia é que o proprietário do smartcard leve a chave até o computador onde deseja usá-la para o ciframento ou deciframento de dados.

Para sistemas de informações, no entanto, são mais indicados os módulos criptográficos, pois além de permitir o seu vínculo físico às instalações onde o sistema executa, tem uma série de requisitos funcionais e de desempenho que o smartcard não possui. Entre os requisitos pode-se citar o rastreamento do ciclo de vida de uso das chaves criptográficas e a execução segura de código. Quanto ao desempenho, a taxa

de ciframento de mensagems pelo módulo é muito superior a taxa que um smarcard consegue realizar. Com a tecnologia atual, um smartcard consegue uma taxa de ciframento de uma ou duas mensagens por segundo. Já um módulo de segurança criptográfica, essa taxa pode alcançar milhares de mensagens cifradas por segundo.

Devido a natureza sensível dos dispositivos criptográficos, em termos de segurança e confiança por parte de seus usuários, organizações e governos de vários países tem regulado como esses dispositivos devem produzidos e utilizados. Normas tais como a FIPS 140-2 (NIST, 2001) do governo americano, especificam as funcionalidade de hardwares criptográficos. Além disso, há entidades credenciadas que verificam se um determinado dispositivo criptográfico está em conformidade com essas normas. E se for o caso, emitem um parecer ou atestado de conformidade.

Um usuário, de posse deste atestado, teria a garantia de que o dispositivo funciona conforme o especificado pela norma, e portanto, poderia confiar que suas chaves criptográficas não seriam indevidamente utilizadas.

Entretanto, apesar da existência de tais conjuntos normativos e do atestado de conformidade, existem uma série de aspectos que precisam ser levados em consideração, para que o usuário possa efetivamente confiar e ter a garantia de que suas chaves criptográficas estejam devidamente protegidas.

Um dos aspectos mais críticos é o relacionado à auditoria do uso da chave e do dispositivo propriamente dito. Essa auditoria é necessária para que se saiba quando e quem autorizou o uso de uma determinada chave.

Embora alguns dipositivos criptográficos forneçam dados de auditoria, esta em si não tem sido feita em todo o ciclo de vida desses dispositivos. Por exemplo, a auditoria do projeto do equipamento, a auditoria da fabricação e entrega do equipamento para o usuário, entre outras.

Na literatura existem poucos trabalhos que buscam formalizar e padronizar a auditoria em dispositivos criptográficos. Este trabalho busca preencher esta lacuna na literatura.

1.1 OBJETIVOS

O ciclo de vida de um HSM é composto por uma sequencia de etapas, que iniciam na concepção e projeto do HSM, e terminando no

descarte do dispositivo.

As propostas de melhoria no processo de auditoria devem ser incluídas nas normas de homologação, para que a auditoria forte de HSMs se torne um padrão nos dispositivos.

1.1.1 Objetivo geral

Este trabalho propõe o estabelecimento de um processo de auditoria unificada em HSMs.

Auditoria Unificada: Processo em que a auditoria é executada durante todo o ciclo de vida de um HSM. O processo utiliza trilhas e rastros de auditoria que possibilitam a detecção da utilização indevida do HSM. A trilha de auditoria é gerada em todas as etapas do ciclo de vida, e cada etapa pode utilizar os rastros das etapas anteriores.

1.1.2 Objetivos específicos

Este trabalho busca atingir objetivos específicos que margeiam o objetivo geral:

- Apresentar os tipos de papéis de usuário necessários para a gerência de chaves criptográficas em dispositivos criptográficos;
- Apresentar as etapas do ciclo de vida de dispositivos criptográficos;
- Mapear as etapas do ciclo de vida de chaves criptográficas com o ciclo de vida de dispositivos criptográficos;
- Apresentar vulnerabilidades e possíveis ataques nas etapas do ciclo de vida de dispositivos criptográficos;
- Apresentar formas de deixar rastros de auditoria nas etapas do ciclo de vida de dispositivos criptográficos;
- Unificar a auditoria no ciclo de vida de dispositivos criptográficos, utilizando os rastros de auditoria gerados nas etapas do ciclo de vida;
- Propor alterações nas normas de homologação de dispositivos criptográficos, para contemplar a geração da trilha de auditoria.

1.2 MOTIVAÇÃO

A auditoria em HSMs é pouco tratada na literatura ou é uma questão tratada superficialmente. Em alguns ambientes como o de ICP, a auditoria é necessária para manter a confiabilidade da infraestrutura.

Uma ICP é um sistema criptográfico que utiliza algoritmos criptográficos para manter a segurança da infraestrutura. As chaves criptográficas utilizadas em uma ICP são armazenadas em HSMs, portanto os HSMs são as âncoras de confiança de uma ICP. Os HSMs devem ser incluídos nos procedimentos de auditoria de uma ICP para garantir o seu funcionamento adequado.

Para que um HSM possa ser utilizado em uma ICP, é comum verificar se o HSM está de acordo com certos padrões. Esses padrões se chamam normas de homologação. Neste trabalho são propostas alterações nas normas de homologação, adicionando requisitos que padronizarão a criação de uma trilha de auditoria nos HSMs.

1.3 CONTRIBUIÇÕES

Este trabalho apresenta o ciclo de vida de dispositivos criptográficos e a importância de se gerar dados de auditoria nas etapas do ciclo de vida. Também são apresentados os procedimentos que devem ser adotados para garantir que os dados de auditoria possam ser utilizados para unificar o ciclo de vida de dispositivos criptográficos.

O trabalho busca apresentar um padrão de produção e gerenciamento de dispositivos criptográficos, que possibilita a detecção de falhas nestes dispositivos em qualquer etapa do seu ciclo de vida.

1.4 METODOLOGIA

Para atingir o objetivo do trabalho é necessário entender o ciclo de vida de HSMs e que tipos de usuários executam ações durante as etapas do ciclo de vida.

O ciclo de vida de chaves criptográficas foi utilizado como base para apresentar o ciclo de vida de HSMs. Com a adição de algumas etapas e remoção de outras, o ciclo de vida de chaves criptográficas se torna o ciclo de vida de HSMs.

As normas de homologação de HSMs definem alguns tipos de usuários que operam estes dispositivos. A partir destes usuários, che-

gamos na definição dos tipos de usuários que podem executar as funções disponíveis em um HSM.

Com o ciclo de vida do HSM e seus usuários estabelecidos, foi descrito neste trabalho quais são as vulnerabilidades existentes em cada etapa do ciclo de vida. Para cada uma dessas etapas, existem formas de se prevenir ataques e gerar rastros de auditoria.

Posteriormente é apresentada uma forma de se levar os rastros de auditoria de uma etapa, para as etapas posteriores. Assim, o proprietário de um HSM poderá auditar qualquer uma das etapas a qualquer momento do ciclo de vida.

Finalmente, as funções que geram rastros de auditoria não necessariamente são requisitos nas normas de homologação de HSMs. Este trabalho descreve como inserir requisitos nas normas para que a geração de rastros de auditoria sejam um padrão em HSMs.

1.5 TRABALHOS CORRELATOS

O trabalho de (CARLOS; CUSTODIO; SUTIL, 2008) mostra uma proposta de preservação de chaves a longo prazo. Quanto maior o tempo de vida necessário para a chave, maior será o esforço necessário para manter o rastreamento da chave.

O trabalho de (SOUZA; MARTINA; CUSTóDIO, 2008) comenta uma proposta de auditoria e backup de chaves criptográficas, para garantir a sua utilização adequada e sua continuidade.

Existe uma implementação de protocolos seguros que incluem auditoria, exposto no trabalho de (MARTINA; SOUZA; CUSTODIO, 2007) onde o OpenHSM é apresentado.

As cerimônias em infraestrutura de chaves públicas são tratadas no trabalho de (MARTINA; SOUZA; CUSTODIO, 2009), que mostram maneiras de se realizar cerimônias em vários estágios do ciclo de vida do HSM.

O trabalho de (GALLO; KAWAKAMI; DAHAB, 2011) propõe um framework para desenvolvimento de hardware seguro, para garantir que o desenvolvimento não possuirá falhas tanto de implementação, quanto de segurança.

1.6 ORGANIZAÇÃO DO TRABALHO

O capítulo 2 apresenta conceitos de criptografia, em especial os conceitos necessários para o entendimento deste trabalho e da solução proposta. O capítulo 3 apresenta qual é o papel dos dispositivos criptográficos em ICPs e qual a sua importância. O capítulo 4 classifica o ciclo de vida de um HSM em etapas, citando vulnerabilidades existentes e o ganho do adversário. O capítulo 5 apresenta a proposta de auditoria nas várias etapas do ciclo de vida do HSM. O capítulo 6 apresenta como inserir a prática de auditoria nas normas de homologação de HSMs. O capítulo 7 conclui o trabalho e cita propostas de trabalhos futuros.

2 GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS

2.1 INTRODUÇÃO

Neste capítulo são revisados os conceitos relacionados com o gerenciamento de chaves e a geração de números aleatórios.

A criptografia é uma área do conhecimento relacionada com a proteção de informações. Essas informações são protegidas de entidades que não possuem permissão de acesso a elas, com a ocultação das informações.

As informações que necessitam de proteção são cifradas com algoritmos de criptografia, que por sua vez são utilizados em conjunto com chaves criptográficas para ocultar as informações. As únicas entidades que poderão visualizar as informações cifradas (ocultadas) são as entidades que conhecem a chave criptográfica utilizada com o algoritmo.

Chaves criptográficas possuem um ciclo de vida com etapas e eventos que podem ocorrer com as chaves durante a sua existência. O ciclo de vida de chaves criptográficas definido por Menezes et al. é apresentado na seção 2.2. Neste trabalho não é proposta nenhuma adição ou melhoria ao ciclo de vida de chaves proposto por Menezes.

O entendimento do ciclo de vida de chaves é necessário para entender outro aspecto do trabalho, que é o ciclo de vida de HSMs, assunto tratado em detalhes no capítulo 4. A proposta desse trabalho, a auditoria unificada em HSMs, é baseada na auditoria do ciclo de vida desses dispositivos.

O ciclo de vida de HSMs é baseado no ciclo de vida de chaves criptográficas, portanto é necessário compreender como o processo funciona. A seção 2.3 descreve as etapas do ciclo de vida de chaves proposto por Menezes, porém relacionadas com o usuário do sistema. Essas etapas são descritas em seção separada da seção 2.2 para facilitar o entendimento do leitor, já que as outras etapas são diretamente relacionadas com a chave criptográfica.

A geração de chaves, que é uma etapa do ciclo de vida de chaves (e de HSMs), é uma das etapas que utiliza um componente conhecido como gerador de números aleatórios. A seção 2.4 apresenta como funcionam alguns tipos de geradores de números aleatórios.

2.2 CICLO DE VIDA DE CHAVES CRIPTOGRÁFICAS

Desde sua criação até o momento de sua destruição, uma chave criptográfica passa por vários estágios. A separação do ciclo de vida de uma chave em estágios é importante para que seja possível se definir qual é a proteção necessária em cada um deles.

Esta seção apresenta o ciclo de vida de chaves criptográficas definido por Menezes et al. A figura 1 apresenta o ciclo de vida de chaves criptográficas, a qual apresenta o ciclo de vida de chaves assimétricas, sendo possível utilizá-la para apresentar o ciclo de vida de chaves simétricas, que é mais simples. Menezes explica que o ciclo de vida de chaves simétricas é menos complexo, pois com essas chaves tipicamente não é realizado o registro, backup, revogação e arquivamento (MENEZES et al., 1997).

As etapas que possuem relação com o gerenciamento de usuários do sistema são descritas na seção 2.3; estas etapas são: registro de usuário e inicialização de usuário.

Algumas etapas do ciclo de vida foram fundidas na descrição, pois a separação de tais etapas apenas torna mais complexa a descrição do trabalho e da proposta.

2.2.1 Geração de chave

Esta seção descreve o conjunto de etapas de geração, instalação e registro de chave.

O ponto de partida da existência de uma chave criptográfica é a sua geração. A geração de chave é diferente para cada algoritmo de criptografia utilizado. A geração de chave pode resultar em apenas uma chave, utilizada em algoritmos de criptografia simétrica, ou em um par de chaves, que podem ser utilizadas em algoritmos de criptografia assimétrica.

A chave será utilizada para manter informações em sigilo ou para assinatura digital. A chave pode ser gerada pelo usuário ou pode ser adquirida de um sistema confiável, como um HSM. A chave gerada deve ser instalada no sistema em que será utilizada e associada ao usuário que será o responsável por permitir a utilização da chave.

No processo de geração de uma chave criptográfica um gerador de números aleatórios é um componente utilizado pelo algoritmo de geração da(s) chave(s), componente descrito na seção 2.4. A aleatoriedade da chave deve reduzir a probabilidade de um adversário descobrir

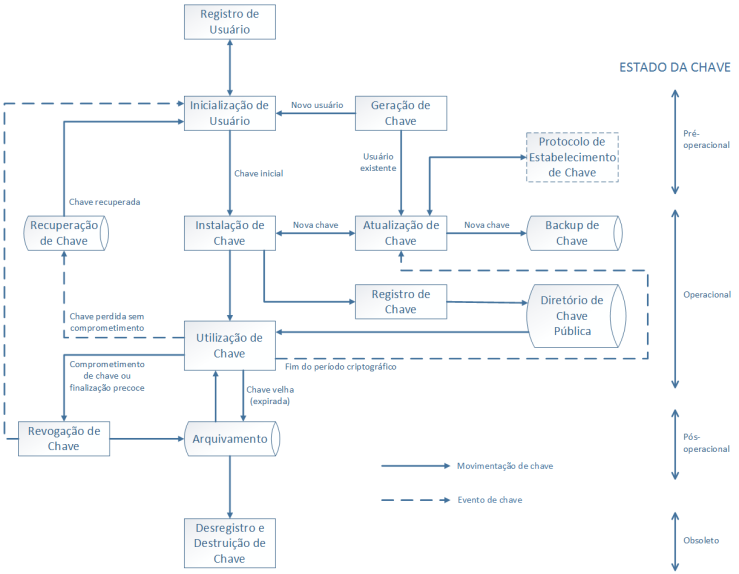

Figura 1: Ciclo de vida de chaves criptográficas (MENEZES et al., 1997)

a chave a um nível em que o ataque seja inviável.

Após a geração da chave, que chamaremos aqui de chave A, essa chave precisa de um local para ser armazenada. A chave criptográfica A pode ser armazenada em claro ou cifrada com um algoritmo criptográfico. Se a chave A for armazenada cifrada, deve existir outra chave criptográfica B para cifrá-la. A chave B pode ser armazenada em memória ou mesmo derivada em tempo de utilização.

Existem implementações de armazenamento onde a chave é armazenada cifrada por um algoritmo de criptografia simétrica que utiliza uma senha para derivar a chave. A senha utilizada pode ser memorizada por uma pessoa. Assim, a chave é armazenada de tal forma que só poderá ser utilizada com a autorização de alguém que conheça a senha.

2.2.2 Utilização

A utilização de uma chave criptográfica é o ato de utilizá-la como o parâmetro em uma função criptográfica. Para a utilização, é necessário conseguir acesso à chave em texto claro. Se a chave foi armazenada

cifrada, é necessário decifrar a chave antes de utilizá-la.

A utilização de uma chave pode possuir políticas de utilização, como período de tempo em que o uso da chave é permitido ou o número de utilizações da chave.

O tempo de utilização da chave pode ser definido quando ela se torna disponível para uso, significando que ela pode ser utilizada por n segundos até que o dispositivo criptográfico não permita mais a sua utilização. O tempo de utilização também pode ser definido por uma faixa de tempo do dia em que é possível utilizar a chave, como por exemplo caixas eletrônicos de banco, onde o caixa não pode ser utilizado em certos horários.

O número de utilizações da chave é definido quando ela se torna disponível para uso, e define quantas vezes a chave pode ser utilizada até que o dispositivo não permita mais a sua utilização.

Assim que a utilização da chave for concluída, é possível armazená-la novamente de forma cifrada para garantir a sua proteção.

2.2.3 Backup

Mecanismos podem ser utilizados para garantir a utilização da chave mesmo na ocorrência de um sinistro que destrua o local onde ela está armazenada. As cópias de segurança são conhecidas como backup.

Assim como no armazenamento, é uma boa prática armazenar o backup de forma cifrada, para impedir o acesso indevido à chave. O armazenamento do backup da chave em outro local impede que a destruição do local da chave destrua o backup também.

O backup de chaves é um problema para a auditoria de chaves. Em uma situação em que o backup de uma chave é restaurado em uma outra instância, é possível que os auditores do sistema não tenham conhecimento desta nova instância. Sem a supervisão dos auditores na nova instância, as chances serão maiores de que um ataque seja bem sucedido.

2.2.4 Destruição

Quando a validade de uma chave expira ou não é mais necessário manter a associação da chave com a entidade que possui o controle de utilização da chave, a chave e todas as suas cópias são destruídas. Ou seja, quando uma chave não é mais útil, ela deve ser destruída.

A destruição de uma chave é mais complicada do que se pode pensar, ou seja, a destruição não significa apenas apagar a chave. Todas as cópias da chave devem ser destruídas, inclusive as cópias de segurança.

A destruição de qualquer atualmente não é um procedimento trivial, portanto podemos dizer o mesmo de uma chave criptográfica.

2.2.5 Recuperação

Na ocorrência de um sinistro onde a chave critográfica armazenada foi perdida, é possível restaurar a chave se as medidas de segurança apropriadas foram tomadas.

A medida de segurança apropriada é o armazenamento do backup da chave, que é utilizado para restaurar a chave.

A recuperação da chave deve ser realizada pela entidade que controla a utilização chave, que pode ser uma pessoa ou um grupo de pessoas, chamados custodiantes. A recuperação é controlada pelos custodiantes, mas os auditores devem ter conhecimento da operação, para verificar se a operação está sendo realizada de forma correta.

2.2.6 Revogação

Uma chave criptográfica pode ser comprometida em algum momento do seu ciclo de vida. O comprometimento de uma chave pode acontecer quando uma chave secreta se torna pública, por exemplo. O comprometimento pode ser causado por um ataque ao sistema ou até mesmo falha de hardware em que a recuperação de backup não é possível.

Quando uma chave criptográfica é comprometida, ela deve ser revogada. Se a chave foi utilizada para assinar certificados digitais, os certificados assinados por esta chave também devem ser revogados.

2.2.7 Arquivamento

Uma chave criptográfica possui um tempo de utilização: a chave expira assim que o tempo de utilização acabar. Uma chave expirada ou revogada deve ser arquivada antes da sua destruição.

O arquivamento de chaves deve ser realizado de forma off-line e é utilizado para resolver disputas que envolvem a irretratabilidade.

2.2.8 Atualização

É necessário que uma chave seja atualizada antes que seu período de utilização termine. A chave é atualizada para que serviços criptográficos que dependem desta chave não sejam interrompidos.

A atualização de uma chave consiste em derivar uma chave criptográfica existente, obtendo uma nova chave. Se um atacante obter acesso à chave antiga e a forma utilizada para derivar, é possível obter a nova chave. Portanto a forma de derivação deve ser mantida em segredo.

2.3 GERENCIAMENTO DE USUÁRIOS

O ciclo de vida de chaves criptográficas proposto por Menezes possui duas etapas que são voltadas para o gerenciamento de usuários das chaves: registro de usuário e inicialização de usuário (MENEZES et al., 1997).

2.3.1 Registro de usuário

Para que uma entidade possa executar operações em um sistema criptográfico que gerencia chaves criptográficas, a entidade deve ser registrada e inicializada no sistema. A execução de operações se refere às etapas descritas na seção 2.2.

O registro de usuário é realizado com a aquisição, criação ou troca de material sensível, como senhas ou PINs (*Personal Identification Number*), através de um canal seguro entre o usuário e o sistema criptográfico (MENEZES et al., 1997).

2.3.2 Inicialização de usuário

A inicialização de um usuário no sistema criptográfico se dá com o envio de material de chave do usuário, material gerado na etapa de registro. O material de chave é diferente de senhas ou PINs, que são dados de autenticação.

A chave criptográfica do usuário pode ser derivada do PIN, utilizando um algoritmo de criptografia simétrica. Essa chave que foi derivada é enviada para o sistema, inicializando o usuário. A chave do

usuário só pode ser utilizada após ser derivada a partir do PIN.

2.4 GERAÇÃO DE NÚMEROS ALEATÓRIOS

O algoritmo de geração de uma chave criptográfica é público. Por este motivo, uma das entradas do algoritmo de geração de chave é um número aleatório, entrada que é necessária para que uma chave seja diferente da outra.

Existem várias formas de geração de números aleatórios. O sistema que gera os números é chamado gerador de números aleatórios (RNG, do inglês *Random Number Generator*).

2.4.1 Gerador de números aleatórios não-determinístico

Uma das características que se espera de uma chave criptográfica, é que a chave seja imprevisível, ou seja, a probabilidade de um indivíduo ou sistema adivinhar qual é a chave gerada por um algoritmo em tempo hábil, deve ser tão pequena que torne o ataque inviável. Por exemplo, para descobrir qual é a chave utilizada em um algoritmo, o adversário levará em média 100 anos, para uma chave que irá expirar em 1 ano.

Para que o resultado da geração de uma chave criptográfica seja imprevisível, é necessário que pelo menos uma das entradas do RNG seja imprevisível. Para isso utilizamos geradores não-determinísticos.

Tipicamente, os geradores não-determinísticos recebem entradas de hardware para decidir se um bit gerado será 0 ou 1.

2.4.2 Gerador de números aleatórios determinístico

Outra forma de RNG é o gerador determinístico, que por exemplo, utiliza algoritmos criptográficos para a geração de números aleatórios. Existem geradores que utilizam algoritmos de HASH ou de criptografia simétrica para determinar qual será um bloco de bits aleatórios.

Um algoritmo de RNG determinístico também recebe entradas. Uma das entradas de um algoritmo de RNG determinístico é a semente. A semente de um RNG é uma entrada aleatória do algoritmo.

Um RNG baseado em HASH recebe a semente como uma das entradas para a geração dos números aleatórios. Os números aleatórios são gerados a partir do HASH da semente recebida combinada com

outro dado como por exemplo, o horário atual no relógio do sistema. Os próximos números aleatórios são gerados a partir do encadeamento do número aleatório gerado anteriormente combinado com a hora atual, neste exemplo. A semente deve ser atualizada após um certo número de encadeamentos, para que os números aleatórios não sejam previsíveis.

A semente pode ser a saída de um algoritmo de RNG não-determinístico (baseado em hardware). Desta forma a entrada aleatória não é prevista. Em casos onde não há a disponibilidade de um RNG não-determinístico para gerar a semente, é possível obter a semente de alguma medida do computador como por exemplo, posição do mouse, teclas pressionadas no teclado, acesso a disco, etc.

2.5 CONCLUSÃO

As contribuições deste capítulo são a apresentação do ciclo de vida de chaves criptográficas proposto por Menezes et al. e a descrição de aspectos que possuem relação com geradores de números aleatórios.

Na seção 2.2 o ciclo de vida de chaves é apresentado, com exceção de duas etapas que são relacionadas com a adição de entidades no sistema. Em seguida são descritas as duas etapas que foram omitidas na primeira seção, etapas que envolvem as entidades que executarão operações no sistema criptográfico, na seção 2.3.

A descrição das etapas do ciclo de vida de chaves criptográficas é necessária para entender os papéis dos usuários de dispositivos criptográficos no capítulo 3. Este capítulo também é necessário para entender as etapas do ciclo de vida de um HSM, também descritas no capítulo 3.

Na seção 2.4 são descritos alguns aspectos dos geradores de números aleatórios. O entendimento destes aspectos é importante para o entendimento do processo de geração de chaves e qual o papel deste componente em um dispositivo criptográfico.

3 DISPOSITIVOS CRIPTOGRÁFICOS

3.1 INTRODUÇÃO

O capítulo 2 descreveu quais são as etapas do ciclo de vida de chaves criptográficas, explicando como a chave criptográfica é gerenciada. Este capítulo busca apresentar quem são os usuários que gerenciam essas chaves e operam dispositivos criptográficos. O capítulo também apresenta alguns tipos de dispositivos, normas de homologação de dispositivos criptográficos, e o ciclo de vida de HSMs em que a proposta desse trabalho se baseia.

O objetivo deste trabalho é realizar a auditoria unificada em HSMs. A proposta consiste em coletar rastros de auditoria durante o ciclo de vida do HSM, e utilizá-los para auditar o que ocorreu em etapas anteriores do ciclo de vida. A proposta é descrita em detalhes no capítulo 5.

Para entender a proposta, é necessário entender melhor o que é um dispositivo criptográfico. Na seção 3.2 deste capítulo está descrito como as chaves criptográficas são gerenciadas em um dispositivo criptográfico, apresentando dois tipos de dispositivos: smartcard e HSM.

A padronização da auditoria unificada também faz parte da proposta deste trabalho. A padronização consistem em adaptar as normas de homologação, para que essas possuam requisitos que possibilitem a auditoria unificada em HSMs homologados. A seção 3.3 descreve o que são as normas de homologação e quais são os órgãos que regulam o seu funcionamento. O capítulo 6 explica em detalhes a adaptação das normas.

Nessa seção, em que as normas são explicadas, são apresentadas duas normas e padrões existentes para possibilitar a interoperabilidade entre dispositivos criptográficos. Os padrões são importantes, pois são eles que definem quais são os requisitos necessários para que um dispositivo possa gerenciar chaves em segurança.

As normas de homologação definem tipos de usuários que devem operar HSMs, e existem trabalhos que propõem outras formas de se operar HSMs, com outros tipos de usuários. Na seção 3.4 deste capítulo, os tipos de usuários que operam um dispositivo criptográfico são apresentados, nas classificações das normas de homologação e Martina et al.

O tipo de usuário que foi apresentado no capítulo 2 na descrição do ciclo de vida de chaves, é um usuário que possui a custódia da

chave, ou seja, a entidade que dará permissão para utilizar a chave. Neste capítulo serão apresentados os outros tipos de usuários que desempenham papéis diferentes em um dispositivo criptográfico. Esses tipos de usuários executam funções e participam em etapas específicas do ciclo de vida de HSMs.

É necessário entender quais são os tipos de usuários de HSMs para compreender qual usuário é o responsável pela auditoria do HSM. É esse tipo de usuário que deverá reunir o material necessário para se unificar a auditoria em um HSM.

A auditoria unificada é uma proposta que utiliza o ciclo de vida de HSMs, para reunir os artefatos de auditoria necessários. Portanto é necessário compreender o que é esse ciclo, e definir quais são as suas etapas. O ciclo de vida de módulos de segurança criptográfica (HSM) em que a proposta se baseia, é apresentado na seção 3.5.

Cada etapa desse ciclo de vida possui certos tipos de usuários que podem executar funções. A seção 3.6 apresenta o relacionamento entre as funções que podem ser executadas por cada tipo de usuário do HSM para cada etapa do ciclo de vida de chaves e HSMs. Os tipos de usuários apresentados na seção 3.4 são comparados para entender as similaridades entre as duas propostas de classificação de usuários.

3.2 DISPOSITIVOS CRIPTOGRÁFICOS

O computador ou dispositivo onde a chave é gerada, armazenada e utilizada interfere em fatores como segurança da chave e performance na sua utilização. Para tornar o uso de algoritmos criptográficos mais eficiente nestes quesitos, utilizam-se dispositivos criptográficos.

No estágio de armazenamento da chave, é importante protegê-la do acesso indevido utilizando proteções físicas. O grau de proteção da chave está diretamente relacionado ao número de proteções utilizadas.

A geração e utilização da chave são estágios que envolvem processamento criptográfico para utilização das funções de criptografia e geração de números aleatórios. Dispositivos criptográficos podem possuir processadores que foram produzidos apenas para estas funções, e portanto são mais eficientes para geração e utilização das chaves.

Existem dispositivos especializados apenas na proteção das chaves, especializados apenas na performance de utilização e/ou geração, e dispositivos que são especializados em ambos. Dispositivos que melhoram o desempenho de funções criptográficas são chamados aceleradores criptográficos.

3.2.1 Smartcard

Smartcards, ou cartões inteligentes, tem como uma das formas de utilização a autenticação onde é necessária a posse de algo. Os cartões de banco são um exemplo dessa forma de autenticação.

A utilização de um smartcard está condicionada à utilização de uma leitora de smartcards, que é responsável por enviar e receber dados do cartão. Outra função da leitora é a alimentação elétrica do smartcard, pois esta é a única interface existente para alimentação do cartão.

As proteções físicas de um smartcard são bastante limitadas quando comparadas com as proteções de outros dispositivos criptográficos. Smartcards não possuem sensores de acesso físico, variações de temperatura, tensão, entre outros tipos de ataques.

A performance de um smartcard também é prejudicada pelo seu tamanho, pois o processador tem um clock limitado e realiza um número baixo de operações por segundo.

A vantagem deste dispositivo é a sua praticidade, pois ele é pequeno o suficiente para ser carregado para qualquer lugar. Alguns exemplos de setores onde é comum a utilização de smartcards é no controle de acesso de funcionários, no transporte público e no setor bancário (cartões de crédito).

3.2.2 HSM

O HSM (*Hardware Security Module* ou Módulo de Segurança Criptográfica) é um dispositivo criptográfico que possui mecanismos de software e hardware para a proteção das chaves criptográficas. O nível de proteção das chaves em um HSM é maior que a proteção oferecida por um smartcard.

Um HSM possui uma área física protegida por sensores, área chamada de perímetro criptográfico. Um HSM possui sensores capazes de detectar tentativas de intrusão e acesso ao perímetro criptográfico, ou variações atípicas de temperatura e tensão. Se os sensores do HSM detectarem a tentativa de intrusão no perímetro criptográfico, todo o conteúdo do HSM é destruído, para evitar o comprometimento das chaves criptográficas contidas no dispositivo.

Um HSM pode ser projetado para ser acoplado à placa mãe de um computador, pela interface PCI por exemplo. Mesmo sem possuir alimentação de energia própria, um HSM desse gênero possui vários

chips e processadores à sua disposição.

Outra forma de projetar um HSM é na forma de um equipamento *stand alone*, ou seja, pode ser ligado e operado sem a utilização de um computador.

Como módulos de segurança criptográfica são mais robustos que cartões inteligentes, eles tendem a ser utilizados em ambientes onde a ocorrência do comprometimento da chave é mais custosa, por exemplo no roubo da chave de uma autoridade certificadora.

HSMs também são mais interessantes em locais onde o ambiente é hostil e possui fraco controle de acesso, por exemplo em caixas de banco.

3.3 NORMAS DE HOMOLOGAÇÃO

Uma norma de homologação é um conjunto de requisitos que devem ser seguidos para que um produto seja certificado, indicando que este produto respeita as normas estabelecidas por aquele conjunto de requisitos.

Nesta seção são apresentadas duas normas de homologação, a FIPS 140-2 e o MCT 7. Entende-se que dispositivos criptográficos que respeitam os requisitos definidos por estas normas, possuem o mínimo de funções necessárias para garantir a segurança de chaves criptográficas. Estas normas também atuam como padronizadores de funções e APIs, tornando os dispositivos homologados interoperáveis entre si.

3.3.1 FIPS 140-2

A FIPS 140-2 é uma norma de homologação de dispositivos e bibliotecas criptográficas. A FIPS 140-2 foi criada pelo CMVP (*Cryptographic Module Validation Program*), que é um programa formado pelo NIST (*National Institute of Standards and Technology*) e pelo CSEC (*Communications Security Establishment Canada*).

Como a FIPS 140-2 define requisitos de vários tipos de artefatos de segurança, podem ser homologados por essa norma: smartcards; HSMs; bibliotecas criptográficas.

Nos EUA e no Canadá, um dispositivo criptográfico só pode ser utilizado em órgão governamentais se tal dispositivo possuir certificado de homologação FIPS 140-2.

No mundo, a norma FIPS 140-2 é uma das normas mais seguidas

por fabricantes de dispositivos criptográficos e também por entidades que desejam adquirir um dispositivo criptográfico.

3.3.2 MCT 7

O MCT 7 (Manual de Condutas Técnicas) é uma norma de homologação, assim como a FIPS 140-2, porém é uma norma brasileira. O MCT 7 foi criado pelo ITI (Instituto Nacional de Tecnologia da Informação), e esta norma é considerada a mais importante no contexto da ICP-Brasil (Infra-estrutura de Chaves Públicas Brasileira).

A ICP-Brasil é uma ICP (Infraestrutura de Chaves Públicas) que é controlada pelo ITI, e documentos eletrônicos assinados com certificados digitais ICP-Brasil possuem valor legal no Brasil.

Para que um dispositivo criptográfico possa ser utilizado na ICP-Brasil, é necessário que este dispositivo seja homologado e respeite os requisitos da norma MCT 7.

O MCT 7 é uma norma criada especificamente para a homologação de HSMs. Existem outros MCTs para a homologação de token criptográficos, bibliotecas criptográficas, software de gerenciamento de certificados, entre outros.

3.4 PAPÉIS DE USUÁRIOS DE DISPOSITIVOS CRIPTOGRÁFICOS

Um dos aspectos de gerenciamento dos dispositivos criptográficos que é padronizado pelas normas de homologação, é a classificação de usuários que operam os dispositivos, separando-os em papéis de usuário. Os papéis de usuário são descritos na seção 4.3.1 da FIPS 140-2 e no requisito III.3.3 do MCT 7.

Os papéis de usuário e funções que podem ser executadas por cada papel existem para definir que tipos de privilégios os operadores do HSM possuirão.

3.4.1 Oficial de segurança

O oficial de segurança é o papel de que tem a função de gerenciar o HSM. A FIPS 140-2 se refere ao oficial de segurança como *crypto officer*.

Este papel de usuário também existe no padrão PKCS#11, po-

rém com o nome *security officer*. O PKCS#11 é um padrão para comunicação entre a aplicação que utiliza serviços criptográficos e o provedor dos serviços criptográficos (HSM ou smartcard).

A FIPS 140-2 e o MCT 7 possuem a mesma descrição de funções do oficial de segurança. As normas descrevem o papel como responsável por: iniciar o HSM; importação chaves; exportar chaves; execução de funções de auditoria; gerenciamento do HSM e; inicialização criptográfica.

O MCT 7 aprofunda no requisito III.3.7, onde descreve que o oficial de segurança deve ser capaz de: inicializar o HSM; gerar chaves RSA; sobrescrever chaves criptográficas com zeros; finalizar o HSM; executar auto-testes e; requisitar informações de estado do HSM.

3.4.2 Usuário

O papel de acesso descrito nesta seção vem da tradução literal da FIPS 140-2, de "*user role*". O papel usuário é capaz de utilizar as funções criptográficas do HSM, como assinatura, cifragem e decifragem.

O MCT 7 também descreve melhor quais funções o papel de acesso usuário deve poder executar, as funções são:

a) manipulação (leitura, escrita, criação e remoção) de chaves criptográficas;

b) acesso a funções de:

   1. autenticação;
   2. transferência segura de mensagens;
   3. assinatura digital;
   4. cifragem;
   5. decifragem;
   6. geração de HASH;
   7. geração de códigos MAC;

c) geração de chaves RSA;

d) requisição de informação de estado do HSM.

Portanto, entidades com o papel de acesso usuário podem utilizar o HSM e suas funções criptográficas, porém não podem executar tarefas de gerenciamento de usuários ou do próprio HSM, como a inicialização e finalização do dispositivo.

3.4.3 Manutenção

Um HSM pode permitir que seus operadores possam executar funções de manutenção; para estes HSMs é necessária a existência do papel de manutenção.

Entidades que possuem permissão de manutenção podem executar manutenção física e lógica no HSM, como diagnósticos que verificam se o dispositivo está funcionando corretamente.

A FIPS 140-2 não descreve mais nenhuma função específica a respeito do papel de manutenção. O MCT 7 detalha melhor as funções que devem estar disponíveis para os operadores responsáveis pela manutenção no requisito III.3.11. De acordo com o MCT 7, os operadores com o papel de manutenção devem poder realizar: backup de chaves; recuperação de chaves; configuração de operadores; configuração e controle de logs.

Podemos notar que as definições da FIPS 140-2 e MCT 7 sugerem que um HSM que respeita os requisitos das duas normas, deve permitir que o papel de oficial de segurança e manutenção possam realizar o backup, restaurar o backup, gerenciar os grupos do HSM e realizar tarefas de auditoria.

3.5 CICLO DE VIDA DE HSMS

No capítulo 2 foi descrito o ciclo de vida de chaves criptográficas. Na seção 3.4 foi apresentado como as normas de homologação requisitam que os operadores de HSMs devem ser gerenciados, e quais funções cada papel de usuário pode executar.

Na seção 3.5.1, os papéis de operação do HSM serão apresentados de acordo com a definição de (MARTINA; SOUZA; CUSTODIO, 2007), classificando os papéis em grupos. São apresentados os grupos de administração, operação e auditoria.

Com base no ciclo de vida de chaves definido por (MENEZES et al., 1997) e nos papéis de operação definidos por (MARTINA; SOUZA; CUSTODIO, 2007), o ciclo de vida de HSMs é definido na seção 3.5.2.

3.5.1 Papéis de usuários de HSMs

Os papéis de usuários classificados aqui são: administração, operação e auditoria. Nesta proposta, existem grupos que podem possuir

permissão para executar funções de um dos papéis.

Os papéis de usuário estão relacionados com certas funções do HSM, assim como os papéis definidos pelas normas de homologação.

As normas de homologação afirmam que o papel de manutenção é opcional, e deve existir se o HSM provê funções de manutenção. Todos os papéis definidos por (MARTINA; SOUZA; CUSTODIO, 2007) devem existir em um HSM que implementa os grupos desta forma.

3.5.1.1 Administração

O grupo de administradores é formado por usuários que terão a responsabilidade de gerenciar o HSM, gerenciar os grupos de usuários que irão operar o dispositivo e realizar a manutenção do HSM. Só pode existir um grupo de administradores em um HSM. É possível alterar os membros do grupo de administradores para refletir mudanças na equipe de membros que gerenciam o HSM.

Entre as tarefas que são de responsabilidade dos administradores podemos citar:

a) Inicialização e finalização do HSM;

b) Gerenciamento do HSM;

c) Gerenciamento de grupos;

d) Backup de chaves;

e) Recuperação de chaves;

f) Geração de chaves.

Portanto o grupo de administradores é semelhante ao oficial de segurança definido pelas normas de homologação, com duas diferenças:

a) As normas não especificam quantos oficiais de segurança podem existir, portanto podem existir de 1 a N oficiais de segurança. No entanto, o grupo de administradores é único e composto de 1 a N membros, sendo necessária a autenticação de M membros para executar uma operação deste grupo, sendo $M \leq N$;

b) As normas de homologação indicam que tarefas de auditoria devem ser executadas pelo oficial de segurança. O grupo de administradores não executa funções de auditoria, pois esta é uma tarefa do grupo de auditores (detalhado abaixo).

3.5.1.2 Operação

O grupo de operadores é formado por usuários que permitirão que as chaves gerenciadas sejam utilizadas. Um HSM pode possuir vários grupos de operadores, sendo que cada grupo pode conter de 1 a N membros. Esta proposta não permite a alteração de um grupo de operadores: se existir a necessidade de se modificar um grupo de operadores, outro grupo deve ser criado, mantendo o grupo antigo no HSM.

A custódia de uma chave gerenciada pelo HSM pode ser atribuída a um único grupo de operadores; no entanto um grupo de operadores pode possuir a custódia de várias chaves.

Podemos citar algumas funções que podem ser executadas pelo grupo de operadores:

a) Cifragem;

b) Decifragem;

c) Assinatura digital;

d) Cálculo de HASH.

Podemos notar que o papel de usuário definido pelas normas que mais se assemelha ao grupo de operação é o papel usuário. As normas definem que membros do papel usuário deve pode gerar e remover chaves criptográficas, o que é impossível de ser realizado pelo grupo de operadores. Esta proposta considera a geração e remoção de chaves como uma tarefa administrativa, portanto é o grupo de administradores que gera chaves, o grupo de operadores possui permissão apenas de utilizar estas chaves.

3.5.1.3 Auditoria

O grupo de auditores é formado por usuários que verificarão se o HSM está funcionando de forma correta e se as chaves estão em segurança.

As normas de homologação requisitam que o oficial de segurança seja capaz de executar tarefas de auditoria e que o usuário de manutenção seja capaz de configurar e controlar os logs. Nesta proposta, o grupo de auditores executa as tarefas de auditoria e utiliza os logs para verificar se as chaves e o HSM estão em segurança.

Desta forma, o grupo de auditores é capaz de verificar se os grupos de administradores e operadores estão executando suas operações de forma correta. Se algum dos grupos de auditores encontrar alguma irregularidade no HSM, o grupo pode bloquear o HSM para evitar que seu conteúdo seja comprometido. Os logs de auditoria exportados são utilizados para comprovar que existem irregularidades no HSM.

Portanto, o grupo de auditores não tem grande semelhança com nenhum papel definido pelas normas de homologação. As funções do grupo de auditores são divididas entre o papel de oficial de segurança e o papel de manutenção.

3.5.2 Etapas do ciclo de vida

O ciclo de vida de chaves criptográficas proposto por Menezes não pode ser utilizado para descrever o ciclo de vida de um HSM (MENEZES et al., 1997). Nesta seção descrevemos o ciclo de vida proposto para HSMs, iniciando no projeto do dispositivo e concluindo o ciclo de vida no descarte do equipamento.

A figura 2 apresenta a sequência das etapas do ciclo de vida de HSMs.

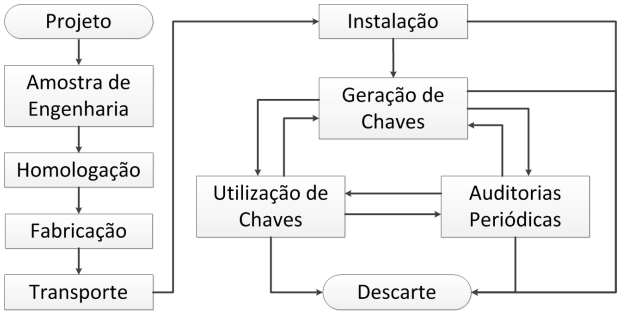

Figura 2: Etapas do ciclo de vida do HSM

As etapas do ciclo de vida de HSMs são:

a) Projeto: modelagem física e lógica dos componentes e do software do HSM;

b) Amostra de engenharia: fabricação de uma ou algumas unidades do HSM, seguindo o que foi definido no projeto;

c) Homologação: envio da amostra de engenharia para homologação;

d) Fabricação: fabricação de HSMs para que sejam distribuídos para os usuários finais;

e) Transporte: envio do HSM para o usuário final;

f) Instalação: inicialização e configuração do HSM, realizada pelo grupo de administradores;

g) Geração de chaves: geração das chaves criptográficas que serão protegidas pelo HSM, realizada pelo grupo de administradores;

h) Utilização de chaves: utilização das chaves para os serviços criptográficos providos pelo HSM, realizada por um grupo de operadores;

i) Auditorias periódicas: exportação de logs e verificação de tentativa de intrusão física no HSM, realizada por um grupo de auditores;

j) Descarte: finalização do HSM, excluindo seu material de chave, realizada pelo grupo de administradores.

3.6 COMPARAÇÃO DE CICLOS DE VIDA E PAPÉIS DE USUÁRIO

A tabela 1 apresenta uma relação entre as funções disponíveis em um HSM, e quais papéis de usuário podem executar cada função.

A comparação tem o objetivo de facilitar a visualização de qual papel de usuário poderá executar as funções, e visualizar a semelhança entre alguns tipos de papéis definidos por autores distintos.

A segunda coluna apresenta os papéis de usuário definidos pelas normas de homologação, os papéis conhecidos como: oficial de segurança, usuário e manutenção. A terceira coluna apresenta os papéis de usuário definidos por (MARTINA; SOUZA; CUSTODIO, 2007), os papéis de: administração, operação e auditoria.

Na tabela comparativa podemos notar as três conclusões obtidas na seção 3.5.1:

a) O papel de administração é semelhante ao papel de oficial de segurança e incorpora boa parte das funções do papel de manutenção;

b) O papel de auditoria executa tarefas de auditoria do HSM e controla de logs de operação, tarefas executadas pelo oficial de segurança e papel de manutenção, respectivamente;

Função	**Normas de Homologação**	**Martina**
Inicialização do HSM	Oficial de Segurança	Administração
Gerenciamento do HSM	Oficial de Segurança	Administração
Criação de usuários	Oficial de Segurança	Administração
Geração de chaves	Oficial de Segurança e Usuário	Administração
Utilização de chaves	Usuário	Operação
Backup de chaves	Manutenção	Administração
Recuperação de chaves	Manutenção	Administração
Tarefas de auditoria	Oficial de Segurança	Auditoria
Exportação de logs	Manutenção	Auditoria
Finalização do HSM	Oficial de Segurança	Administração

Tabela 1: Relação entre funções e papéis de usuário

c) O papel de operação se assemelha ao papel de usuário, porém não pode gerar chaves criptográficas, pois esta é uma tarefa de gerenciamento do HSM e portanto é executada pelo papel de administração.

3.7 CONCLUSÃO

Este capítulo apresentou alguns conceitos que são essenciais para o entendimento do trabalho. A proposta da auditoria unificada é focada em HSMs, portanto o capítulo começa com a descrição do que são os dispositivos criptográficos smartcard e HSM, na seção 3.2.

A adaptação das normas que homologam dispositivos criptográficos também é parte da proposta do trabalho. A adaptação visa incluir requisitos nas normas, que possibilitam a auditoria unificada em qualquer HSM homologado. A seção 3.3 descreve o que são normas de homologação de dispositivos criptográficos.

As normas de homologação apresentadas na seção 3.3 definem alguns tipos de usuários que gerenciam dispositivos criptográficos. Esses tipos de usuários são apresentados na seção 3.4. O entendimento desses usuários é necessário para entender qual é o papel desempenhado por cada usuário no ciclo de vida de um dispositivo criptográfico, em especial HSMs.

A auditoria unificada é realizada durante o ciclo de vida do HSM, sendo necessário reunir certos artefatos dependendo da etapa do ciclo de vida em que o HSM está. A seção 3.5 apresenta aspectos relacionados

ao ciclo de vida de HSMs.

Um dos aspectos importantes na gerência de um HSM, é a classificação utilizada para os tipos de usuários. Neste trabalho adotamos a classificação de Martina et al., que é uma classificação diferente das normas de homologação; a seção 3.5.1 apresenta esta classificação.

O ciclo de vida de HSMs adotado neste trabalho é apresentado na seção 3.5.2, que descreve quais são as suas etapas. Este ciclo de vida será apresentado em detalhes no capítulo 4, descrevendo vulnerabilidades das etapas e quais são os rastros de auditoria que devem ser gerados.

Os rastros de auditoria gerados nas etapas do ciclo de vida são utilizados na unificação da auditoria. Esse processo é descrito no capítulo 5, onde os artefatos de uma etapa podem ser utilizados nas etapas seguintes para validar a auditoria no ciclo de vida do HSM.

A seção 3.6 finaliza este capítulo comparando os tipos de usuários apresentados até então, relacionando os usuários com as funções que podem executar em um HSM. Essa seção demonstra que os tipos de usuário são bastante semelhantes, porém a definição de Martina trata a auditoria como uma atividade separada da gerência de chaves e gerência do HSM.

4 ANÁLISE DO CICLO DE VIDA DE HSMS

4.1 INTRODUÇÃO

O capítulo 3 define e explica o que é o grupo de auditores, que é o grupo responsável por verificar que nenhuma irregularidade ocorreu com o HSM. Irregularidades acontecem em um HSM quando as políticas estabelecidas para a sua utilização são desrespeitadas, sendo que essas políticas são definidas pelo proprietário do dispositivo.

As políticas definidas para utilização do HSM refletem o manuseio do dispositivo após a sua entrega ao proprietário. O proprietário estará com o seu HSM em mãos após ocorrer a entrega por parte da empresa que realizou a venda do HSM. Da mesma forma, a auditoria do HSM só poderá ser realizada após a entrega do HSM.

Da forma como o processo é realizado os auditores não tem como atestar se o HSM sofreu ataques antes de chegar no proprietário, pois o HSM estará em posse do fabricante, órgão de homologação ou transportadora.

A entrega do HSM (transporte) é uma das etapas do ciclo de vida do dispositivo, apresentado na figura 3. Este capítulo descreve em detalhe as etapas do ciclo de vida de um HSM.

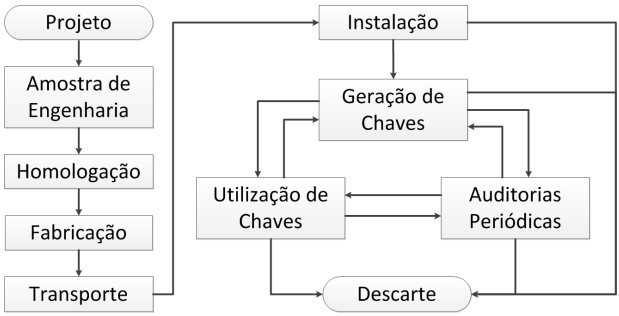

Figura 3: Etapas do ciclo de vida do HSM

Cada etapa do ciclo de vida está suscetível a ataques. Um adversário pode comprometer um HSM em qualquer uma das etapas, inclusive naquelas onde as chaves criptográficas ainda não foram criadas ou estão para ser destruídas.

Diferentes ataques que venham a comprometer um HSM podem possuir impactos diferentes para o proprietário do HSM, sendo a utilização não autorizada de chaves criptográficas o pior impacto. O impacto do ataque é representado pelo ganho do adversário.

O ganho do adversário é uma das especificidades que serão ressaltadas em cada etapa. As especificidades que serão descritas em cada uma das etapas serão:

- **Duração da etapa:** Tempo decorrido entre o início e fim da etapa. O tempo não será descrito com precisão, pois a duração da etapa pode variar de um cenário de utilização do HSM para outro.
- **Ganho do adversário:** Uma forma de se atacar o HSM será apresentada e qual o ganho do adversário no ataque. A forma de ataque apresentada é uma das formas que produzirá o maior impacto negativo para o proprietário do HSM.
- **Recursos necessários:** Alguns recursos são necessários para que um ataque seja bem sucedido. Os recursos que serão listados são referentes ao ataque apresentado com maior ganho do adversário. Os recursos podem ser físicos (hardware), acesso ao HSM, posse de algo relacionado ao HSM, ou autorização para executar uma tarefa específica no HSM.
- **Tempo necessário:** A quantidade de tempo necessária para que o ataque apresentado seja executado. O tempo necessário não será descrito com precisão, pois a duração do ataque pode variar de um cenário de ataque para outro.
- **Trilha de auditoria:** A trilha de auditoria são todos rastros que o HSM pode gerar, utilizados para possibilitar a detecção de que um ataque ocorreu. Durante o processo de auditoria deve ser possível analisar as evidências na trilha de auditoria e detectar quem atacou o HSM e quando o ataque ocorreu. Para que isso seja possível, os rastros de auditoria devem ser precisos e detalhados.

A trilha de auditoria será utilizada pelos auditores para detectar se houve uma intrusão ou tentativa de intrusão no HSM. O trabalho dos auditores é mais simples após a chegada do HSM na instalação física do seu proprietário, pois tipicamente os auditores tem acesso ao HSM e podem realizar as tarefas de auditoria. Antes da chegada do HSM nas mãos do proprietário, é difícil ou impossível que os auditores possam atestar a segurança do HSM.

O detalhamento da trilha de auditoria é vital para o processo de auditoria. Se as operações não forem detalhadas, não será possível saber com certeza o que ocorreu no HSM. Informações detalhadas podem levar à detecção do adversário que atacou o HSM. Informações incertas em um registro de auditoria podem levar ao comprometimento do HSM sem que o adversário possa ser identificado.

Em algumas etapas do ciclo de vida a trilha de auditoria é composta por uma ata das atividades realizadas no HSM. Essas atividades são realizadas em uma cerimônia.

Cerimônia: Evento que possui uma sequência de passos pré-definidos para utilizar o HSM, como inicialização, configuração e utilização.

Roteiro da cerimônia: Sequência de passos que serão executados na cerimônia. O roteiro é definido antes do início da cerimônia.

Log da cerimônia: Ata ou registro de atividades realizadas na cerimônia. Os resultados de cada uma das operações executadas na cerimônia são relatados no log da cerimônia.

Os artefatos gerados na trilha de auditoria, somados ao roteiro e log da cerimônia (quando a etapa exigir a ocorrência de uma cerimônia), formam um conjunto de artefatos que serão utilizados para unificar a auditoria do HSM, processo descrito no capítulo 5. A proposta do trabalho é que seja possível auditar as etapas anteriores do ciclo de vida, utilizando os rastros de auditoria.

As seções deste capítulo descrevem em detalhes as etapas do ciclo de vida de HSMs. A primeira etapa, a etapa de projeto, é descrita na seção 4.2. A seção 4.3 apresenta a etapa de amostra de engenharia. A etapa de homologação é descrita na seção 4.4, a etapa de fabricação na seção 4.5 e a etapa de transporte na seção 4.6. Após a entrega do HSM ao proprietário, inicia-se a etapa de instalação na seção 4.7, seguida pelas etapas de geração de chaves na seção 4.8, utilização de chaves na seção 4.9 e auditorias periódicas na seção 4.10. Por fim, a etapa de descarte do HSM é apresentada na seção 4.11.

4.2 PROJETO

A etapa de projeto do HSM é a primeira etapa do ciclo de vida e o início da fabricação de um HSM, ou de uma série de HSMs.

Uma analogia ao projeto do HSM é a implementação de classes em linguagens de orientação a objetos, como Java. O projeto pode ser

visto como uma classe, que possui atributos e métodos. Os atributos são as características e configurações de HSMs que saem de fábrica. Os métodos são funções do HSM que são executadas, que podem possuir retorno ou não. Posteriormente, a analogia se estenderá para a instanciação das classes, ou seja, para os objetos criados a partir dessas classes, que são os HSMs fabricados.

O projeto do HSM consiste na modelagem física e lógica de componentes e software.

A modelagem física consiste na descrição de como os componentes de hardware serão posicionados no HSM e como a comunicação entre os componentes ocorrerá. Os componentes físicos da modelagem incluem os sensores de intrusão do HSM, que são necessários para detectar e mitigar ataques físicos ao dispositivo.

A modelagem lógica é a descrição do software que coordena as funções executadas no HSM. Esta modelagem inclui diagramas de modelagem de software, como o UML, que são gerados antes da implementação do software do HSM. As proteções lógicas também são descritas, indicando o que é protegido no HSM e como estas são aplicadas.

4.2.1 Duração da etapa

A etapa de projeto tem duração de meses. Esta é a etapa que tipicamente possui a janela de tempo maior para a realização de um ataque.

4.2.2 Ganho do adversário

O ataque nesta etapa do ciclo de vida é a adulteração do projeto. Um adversário pode alterar o projeto, inutilizando um componente que é responsável pelo controle de um ou mais sensores que detectam intrusão física. O adversário também pode inserir um componente que deixará uma abertura nas proteções.

A adulteração do projeto também pode atingir o nível lógico. O adversário pode alterar a modelagem do software removendo proteções na comunicação de dados. Também é possível remover a cifragem de informações para que o conteúdo secreto fique em claro no HSM.

O objetivo do adversário nesta etapa é sabotar o HSM. A sabotagem de um HSM pode permitir ataques no futuro, realizando a cópia de chaves criptográficas armazenadas ou sua utilização não autorizada. A

sabotagem também pode ter como alvo a empresa que fabrica o HSM, para que um dispositivo seja atacado e a empresa seja responsabilizada por produzir um HSM que não protege os dados.

Este tipo de ataque é muito difícil de ser detectado posteriormente, pois os mecanismos de ataque estarão implementados no HSM e sendo protegidos pelo próprio dispositivo. Este tipo de ataque pode ser causado pelo próprio fabricante, para que seja possível roubar chaves criptográficas de seus clientes, os proprietários de HSMs. O ato de deixar aberturas no dispositivo que ele próprio projetou se chama Cleptografia (*Kleptography*), conceito introduzido por Young (YOUNG; YUNG, 1997).

4.2.3 Recursos necessários

Para que o ataque possa ser executado, o adversário deve ter acesso ao projeto do HSM. O acesso ao projeto pode ser conseguido de forma ilícita, sendo esta a situação mais improvável. O acesso ao projeto de alguém que trabalha na empresa que fabrica o HSM é a situação mais simples e provável de se acontecer.

Acesso ao projeto não garante a possibilidade de adulteração. É necessário que o adversário tenha permissão de modificação do projeto para que a adulteração tenha êxito.

O ataque às chaves criptográficas armazenadas acontecerá no futuro, portanto a adulteração e inserção de falha no sistema pode não ser detectada. É necessário que a falha inserida não seja detectada pelo processo de homologação do HSM. Se a adulteração no projeto for detectada, será necessário corrigí-la e o ataque não terá nenhum efeito. Este caso se aplica se o fabricante souber que a falha está sendo inserida.

Se o fabricante não souber que uma falha está sendo inserida, a falha deve ser inserida de tal forma que o fabricante não a perceba.

4.2.4 Tempo necessário

O tempo necessário para adulterar o projeto pode ser muito pequeno, com duração de alguns minutos ou horas no caso ideal. O caso ideal consiste em um adversário que conhece o projeto e tem permissão de modificação, possivelmente sendo alguém que trabalha na equipe que projetou o HSM. Esta pessoa poderia adulterar o projeto com uma

chance maior de a modificação passar despercebida pelo fabricante e pela homologação do HSM.

O tempo necessário pode ser de vários meses quando o adversário conhece pouco sobre o projeto. Um adversário que possui permissão para modificar o projeto e não faz parte da equipe que projetou o HSM, deverá estudar o projeto e procurar o local onde a falha será inserida.

4.2.5 Trilha de auditoria

O projeto do HSM deve ser armazenado em um sistema de controle de versão. Este sistema de controle de versão deve registrar todas as alterações realizadas no projeto, quem realizou a alteração e quando a alteração foi realizada. Cada versão (ou revisão) do projeto deve conter comentários do que foi alterado no projeto.

O controle de versão do projeto auxilia na verificação do responsável pela inserção de uma falha no HSM. Uma falha inserida no projeto será utilizada futuramente, quando o HSM estiver em funcionamento e gerenciando chaves criptográficas. Com as alterações de projeto registradas, é possível verificar quem foi a pessoa que realizou a alteração e possivelmente detectar se a falha foi inserida de forma proposital.

Um adversário pode modificar o projeto e excluir o registro da modificação no sistema de controle de versão, ou alterar os detalhes da modificação. Os detalhes alterados podem ser o nome pessoa que modificou o projeto e a data da modificação, para esconder o rastro da modificação mal intencionada. O sistema de controle de versão deve ser protegido para evitar que os rastros sejam perdidos. As proteções podem ser de modificação no sistema, exclusão de dados utilizando cópias de segurança e adição de informações incorretas.

4.3 AMOSTRA DE ENGENHARIA

A amostra de engenharia é a primeira versão ou algumas versões produzidas seguindo o projeto do HSM. A amostra serve para verificar que o projeto descreve um HSM com as proteções que o fabricante desejava que o dispositivo fosse capaz de implementar.

Testes das proteções físicas e lógicas são realizados na amostra para verificar se as proteções foram implementadas de acordo com o projeto. Usualmente a amostra não é comercializada ou utilizada em ambiente de produção.

O fabricante deve atestar que a amostra de engenharia implementa o que foi descrito no projeto. Se a amostra for alterada por qualquer motivo, o projeto deve ser modificado para representar a nova implementação. O motivo de alteração da amostra de engenharia pode ser uma falha encontrada ou alguma proteção que foi aprimorada.

4.3.1 Duração da etapa

A amostra de engenharia leva meses para ser montada. O tempo de montagem consiste no tempo necessário para reunir as peças de hardware utilizadas e implementação do software do HSM.

Na prática o hardware é adquirido e o software é implementado à medida que o projeto é desenvolvido. Algumas partes do projeto podem possuir pouca probabilidade de serem alteradas futuramente, estas partes podem ser implementadas antes que o projeto seja concluído. Com um bom gerenciamento do projeto o tempo de montagem da amostra pode ser reduzido.

4.3.2 Ganho do adversário

O adversário atacará o HSM fabricado como amostra de engenharia nesta etapa.

Voltando para a analogia descrita na etapa de projeto, a amostra de engenharia é uma instância do projeto do HSM. A amostra, uma instância do projeto, não tem potencial para ser utilizada em ambiente de produção. Um ataque em um HSM que não será utilizado para gerenciar chaves não terá nenhum impacto para as chaves ou algoritmos. O ataque nesta etapa é direcionado para o fabricante do HSM.

O adversário nesta etapa irá inserir falhas no HSM para que o dispositivo não seja aprovado pelo órgão de homologação. O adversário alterará o protótipo para que seja suscetível a ataques e que os ataques sejam detectados pelo órgão de homologação. Desta forma a empresa fabricante do HSM não conseguirá a homologação ou o processo será atrasado, pois a falha terá que ser corrigida antes que a homologação possa ser concedida.

4.3.3 Recursos necessários

A janela de tempo onde o ataque ocorre precisa estar durante a montagem da amostra de engenharia. A inserção da falha no hardware do HSM deve ser realizada enquanto o HSM está em fase de montagem e união da eletrônica do dispositivo. A falha inserida em software deve acontecer durante a implementação do software de gerenciamento do HSM.

O adversário que irá inserir a falha no HSM deve ter acesso ao dispositivo durante a montagem da amostra. O ataque acontecerá de forma mais rápida e simples se o adversário trabalhar na empresa que fabrica o HSM. O ataque se torna mais sutil se o adversário fizer parte da equipe de implementação do software ou montagem do HSM.

4.3.4 Tempo necessário

O tempo necessário para realizar o ataque varia bastante. O adversário que trabalha no desenvolvimento do HSM, irá inserir uma falha em questão de minutos. O adversário que tem acesso ao HSM, porém não trabalha no desenvolvimento do dipositivo, levará dias para encontrar como inserir a falha e o momento certo de inserir.

Uma forma simples para o ataque é explorar uma falha que já existe no HSM, mas que não é uma falha visível. O adversário pode criar uma forma de tornar a falha visível ao órgão de homologação.

O caso mais complicado é a situação em que o adversário não tem acesso ao HSM ou ao seu projeto. O adversário terá que conseguir o projeto do HSM, estudá-lo para encontrar uma maneira de se inserir a falha, para depois inserir a falha no HSM. Esse ataque requer muito tempo para ser realizado, possivelmente levando meses para realizar o ataque sem ser detectado.

4.3.5 Trilha de auditoria

O ataque nesta etapa acontece em um dispositivo único, ou seja, em um HSM que é a amostra de engenharia. Portanto o HSM que é a amostra deve ser monitorado para detectar modificação não autorizada durante a montagem.

A adulteração de software pode acontecer com a inserção de um firmware malicioso na montagem do dispositivo. O firmware do HSM

deve passar por um teste de integridade antes de ser inserido no HSM. O teste de integridade deve utilizar uma função de HASH aplicada ao software, e o resultado da função de HASH deve ser guardado para conferência em caso de necessidade no futuro.

Não é possível utilizar o hardware como entrada em uma função de HASH, portanto a montagem do HSM deve ser documentada. O fabricante deve registrar os componentes inseridos na eletrônica do HSM, para conferir posteriormente se não houve adulteração de componentes.

O registro de quem teve acesso à amostra de engenharia é tão importante quanto o registro de quais componentes de software e hardware foram inseridos no HSM. Se o adversário inserir uma falha no HSM, e esta pessoa não possui autorização para acessar ou manusear o HSM, é provável que esta pessoa tenha agido de forma maliciosa. O registro de acesso irá facilitar a investigação de quem inseriu a falha.

4.4 HOMOLOGAÇÃO

Nesta etapa o fabricante submete seu HSM para um órgão de homologação, junto com outros artefatos relacionados ao HSM, como o projeto. O fabricante faz o pedido de homologação para receber o certificado de que o HSM está de acordo com o padrão estabelecido pelo órgão. Os fabricantes submetem o HSM a um órgão homologador para aumentar a sua aceitação no mercado e comprovar que o dispositivo atende a requisitos de segurança.

Infraestruturas de chaves públicas (ICP) são um exemplo de entidade que utiliza HSMs. As ICPs possuem interesse em utilizar HSMs que passaram pelo processo de homologação de um órgão confiável. A norma de homologação de HSMs que é mais conhecida e utilizada em ICPs é a FIPS 140-2.

4.4.1 Duração da etapa

A duração da etapa de homologação é o tempo necessário para o órgão homologador analisar o HSM e emitir o certificado de que o dispositivo foi homologado, ou o comunicado de que o HSM não está em conformidade com a norma.

O processo de análise do HSM e emissão do resultado da homologação leva meses para ser concluído.

4.4.2 Ganho do adversário

O alvo do adversário na etapa de homologação é o órgão que homologa o HSM. Um órgão de homologação que certifica um HSM com falhas, perde a credibilidade. Fabricantes e compradores de HSMs não terão a mesma confiança no órgão de homologação se este ataque for bem sucedido.

O adversário tentará induzir o órgão de homologação a certificar um HSM com uma falha grave. A falha no HSM impossibilitaria a certificação seguindo o processo de homologação de forma correta. A homologação de um HSM com falhas deixa o fabricante com a falsa sensação de que o dispositivo é seguro.

Para induzir o órgão de homologação a emitir um certificado para um HSM com falhas, o adversário deve participar do processo de homologação. Para participar da homologação, o adversário deve ter contato com o órgão homologador ou deve ser um dos técnicos que avaliam o HSM. Desta forma, o adversário conseguirá ignorar uma falha existente em um dispositivo.

A falha no HSM pode ter sido criada ou inserida na etapa de projeto ou na amostra de engenharia. Falha inserida na montagem da amostra de engenharia não possui o efeito de prejudicar o órgão de homologação, pois a amostra é apenas uma instância do projeto. A falha deve ser inserida no projeto do HSM, assim todos os HSMs construídos possuirão a falha.

A falha no HSM pode existir por erro da equipe de projeto do HSM ou pode ter sido inserida por um contato do adversário que inseriu a falha na etapa de projeto. O adversário no órgão de homologação deve ignorar a falha e atestar que o HSM é seguro.

4.4.3 Recursos necessários

O adversário necessita ter contato com alguém que faça da parte da equipe de avaliação de HSM do órgão homologador, ou ele próprio deve fazer parte da equipe.

A ação do adversário será mais simples e sutil se a falha no HSM for causada por engano do fabricante. No caso da falha ser inserida de forma proposital, a comunicação do adversário com alguém que projeta o HSM é necessária, para que esta pessoa insira a falha que será ignorada pelo adversário no momento da avaliação do HSM.

4.4.4 Tempo necessário

O tempo necessário para executar o ataque é mínimo. O adversário estará executando suas atividades normais na avaliação do HSM e encontrará a falha. A falha será ignorada ou escondida pelo adversário. Portanto, o ataque em si não possui um espaço de tempo definido.

4.4.5 Trilha de auditoria

O órgão de homologação precisa registrar atividades específicas de avaliação de HSMs. As atividades devem conter quem era o avaliador e qual o dia e horário da avaliação, para que o registro seja preciso. Dessa forma será possível detectar qual avaliador deixou uma falha passar na homologação. O registro de atividades apenas descobrirá quem deixou passar uma falha, não evitará a homologação de um HSM com falhas.

Existe uma prática que pode ser adotada pelo órgão homologador para evitar que a homologação de HSM com falha ocorra. O órgão homologação pode possuir equipes diferentes para homologação do mesmo HSM. A homologação de um HSM só poderá ocorrer com a aprovação de duas equipes distintas e sem contato uma com a outra.

Com duas equipes distintas o ataque seria detectado por pelo menos uma das equipes. O adversário teria que possuir um contato na outra equipe, para que a falha possa ser ignorada pelos dois lados.

4.5 FABRICAÇÃO

HSMs que saem de fábrica prontos para ser distribuídos são chamados HSMs de produção. A fabricação de HSMs de produção é realizada de forma diferente da montagem da amostra de engenharia. Os HSMs de produção são fabricados em lotes de vários dispositivos, para reduzir os custos de montagem.

Os HSMs fabricados são instâncias do projeto do HSM, portanto, estes dispositivos possuem as mesmas proteções da amostra de engenharia. Os HSMs de produção são considerados dispositivos homologados pelo órgão de homologação ao qual a amostra de engenharia foi submetida.

O processo de fabricação está sujeito a modificação por parte do fabricante ou de seus funcionários, para tornar o processo mais eficiente

ou barato. Se a alteração da forma como os HSMs são fabricados não é documentada, aumenta a probabilidade de ocorrerem ataques ao HSM durante a fabricação. A padronização do processo de fabricação dificulta a ação do adversário.

4.5.1 Duração da etapa

A montagem de um HSM usualmente está ligada à fabricação de um lote de HSMs. É possível que certas partes da montagem sejam realizadas de forma manual, aumentando a duração da etapa. Não são montados muitos HSMs em um lote, por isso é possível que algumas etapas sejam manuais.

A fabricação de um lote de HSMs leva algumas semanas para ser concluída.

4.5.2 Ganho do adversário

O alvo do adversário na etapa de fabricação são todos os HSMs montados, inserindo falhas em todo o lote de HSMs fabricados. O ataque acontece de forma parecida com um ataque na etapa de projeto, a diferença é que o ataque no projeto prejudica todas as instâncias do projeto. O ataque na etapa de fabricação prejudicará um ou mais lotes de HSMs montados.

O adversário atacará substituindo algum componente do lote de HSMs por um componente defeituoso. A substituição pode levar o adversário a atacar HSMs e conseguir controle total do dispositivo. O componente pode ser o firmware contendo o software interno dos HSMs ou algum componente de hardware que é vital para a segurança dos HSMs.

A substituição de um componente de software requer que o adversário consiga acesso ao software definido no projeto e possa alterá-lo. O software interno do HSM é gravado na memória persistente do dispositivo durante a fabricação, ou o software é inserido durante a montagem do HSM. Se os arquivos contendo o software forem modificados para conter software malicioso, os HSMs estarão abertos para que o adversário possa atacá-lo.

A substituição de componentes de hardware não necessariamente requer que o adversário estude o projeto, mas não estudar o projeto com certeza tornará o ataque mais difícil.

Um tipo de ataque em que o alvo é o componente de hardware é o Hardware Trojan (TEHRANIPOOR; KOUSHANFAR, 2010). Um trojan de software é um software que executa suas tarefas normalmente da forma que o usuário esperava, porém ele deixa aberturas no computador do usuário. O trojan de hardware utiliza o mesmo conceito do trojan de software, funcionando da mesma forma que o componente original, mas deixando aberturas. O trojan neutraliza alguma proteção do HSM, para que o dispositivo fique vulnerável a pelo menos um tipo de ataque.

Um exemplo é a substituição do gerador de números aleatórios (RNG) por um gerador de entropia baixa. Um RNG de entropia alta reduz a previsibilidade dos números gerados, ou seja, é mais difícil descobrir qual é a chave gerada pelo HSM. O adversário pode descobrir qual é a chave criptográfica gerada pelo HSM se o RNG possuir baixa entropia. A substituição do RNG pode ser realizada em software ou hardware, substituindo o gerador de números aleatórios determinístico e não-determinístico respectivamente.

A falha deixada nos HSMs fabricados pode ser explorada futuramente, quando o HSM estiver em uso.

4.5.3 Recursos necessários

Gallo et. al descreve em seu trabalho o *secure device epoch* (SDE) que está relacionado ao processo de fabricação do HSM (GALLO; KAWAKAMI; DAHAB, 2010). Existe um momento na montagem do HSM em que todos os componentes da eletrônica interna já foram inseridos e conectados e o dispositivo será selado. O HSM é selado quando as contramedidas do dispositivo começam a funcionar. O partir do momento em que o HSM é selado, o SDE inicia.

Qualquer visualização e manuseio da parte interna do perímetro criptográfico é considerada uma invasão, ou seja, um ataque. Portanto, um dos recursos necessários é que o adversário execute seu ataque antes que o SDE inicie, pois o perímetro criptográfico ainda estará aberto e suscetível ao ataque na etapa de fabricação.

Acesso físico ao HSM ou aos componentes do HSM é necessário. O acesso físico aos componentes do HSM é suficiente pois a substituição dos componentes por outros que se pareçam com os originais enganará a equipe que os montará. Se o ataque for executado de forma sutil, a equipe estará manuseando componentes sem notar que são maliciosos.

O último recurso necessário é conhecimento do projeto do HSM. Para que o adversário possa saber qual componente deve ser substi-

tuído, ele deve saber qual é o papel dos componentes no sistema. Um adversário que não tem acesso ao projeto tem baixa probabilidade de substituir um componente e manter o HSM funcional.

4.5.4 Tempo necessário

O tempo para substituição do componente é pequeno, o que aumenta o tempo necessário é o conhecimento do HSM que o adversário possui.

O adversário que não conhece o projeto, deverá estudar o projeto, produzir ou conseguir o componente malicioso e encontrar o local onde o componente será inserido. Esse ataque pode levar semanas.

O adversário que trabalha na empresa e conhece o projeto possuirá muito mais facilidade em inserir o componente, podendo executar o ataque em questão de minutos.

4.5.5 Trilha de auditoria

A forma de se verificar se componentes foram substituídos é checar a integridade de cada componente antes de ser inserido no HSM. A verificação é complicada, pois não existem soluções para integridade de hardware. A integridade de software pode ser garantida utilizando funções de HASH.

Para garantir que os HSMs serão produzidos com os componentes corretos, o fabricante deve analisar os componentes de hardware adquiridos para verificar se não são defeituosos. Esta precaução não impede que um adversário substitua o componente de um HSM em específico, porém a substituição dificilmente ocorrerá no lote inteiro.

Uma equipe de montagem de HSMs com pessoas diferentes trabalhando na montagem de partes específicas dos dispositivos, reduz a chance de um adversário atacar um lote inteiro de HSMs.

Outro método é a checagem de HSMs por amostragem, ou seja, garantir que um número de dispositivos é seguro em um lote de HSMs. Quando o comprador de um HSM tem uma importância maior, é possível verificar a segurança deste HSM antes de enviar ao cliente. A checagem dos dispositivos deve ocorrer antes do SDE, pois acessos à eletrônica de um HSM após o SDE é caracterizado uma violação ou ataque físico ao HSM.

Não existem soluções genéricas ou um meio genérico de realizar

a auditoria na etapa de fabricação de HSMs, por isso são necessárias várias precauções na montagem dos HSMs. Esta é uma das etapas onde os HSMs estão mais vulneráveis.

4.6 TRANSPORTE

Uma das características que auxilia na proteção de um HSM é o local onde o dispositivo é mantido e quem tem acesso a ele. Nas etapas anteriores o HSM estava nas mãos do fabricante, que deve zelar pela segurança física do dispositivo. O fabricante envia o HSM para seu cliente (proprietário do HSM), assim o dispositivo passa a entrar na etapa de transporte, onde o HSM não estará nas mãos nem do fabricante, nem do proprietário do HSM.

O desafio desta etapa é garantir que o HSM fabricado é o mesmo que está sendo entregue ao proprietário, sem modificações. Como a pessoa ou empresa que realiza o transporte do HSM tem acesso total ao dispositivo durante o envio, um adversário na transportadora terá um dos recursos necessários para o ataque. Podemos notar na maior parte das etapas do ciclo de vida, o acesso físico ao HSM é um recurso necessário para ataques.

A transportadora não faz parte de nenhum dos grupos que podem ser confiados no ciclo de vida do HSM. Os grupos que podem ser confiados são os proprietários do HSM (representados pelos auditores), fabricante e órgão de homologação. A transportadora tem contato com o HSM quando ele transita entre o fabricante e o proprietário. Para a homologação, consideramos que o fabricante leva as amostras em mãos para o órgão de homologação.

4.6.1 Duração da etapa

O transporte de um HSM envolve logística da empresa que fabricou o dispositivo, da transportadora e do proprietário do HSM. Quanto maior a quantidade de HSMs a serem enviados mais tempo os dispositovs levarão para chegar ao destino. A distância geográfica é o fator que pode ser calculado mais facilmente e que também interfere no tempo de envio, desde que se saiba qual é o meio de transporte utilizado, que é outra variável do processo.

Como o transporte envolve todas estas variáveis e possivelmente outras que estão fora do escopo deste trabalho, não podemos calcular

o tempo de duração da etapa de transporte.

4.6.2 Ganho do adversário

O adversário modificará ou substituirá o HSM que está sendo enviado para o proprietário.

A modificação pode ser de algum componente do HSM, como o firmware ou componentes da eletrônica que são essenciais para a segurança física do equipamento. O ataque é sofisticado, pois o adversário deve modificar o HSM sem que o dispositivo indique violação física e sem deixar vestígios. O ataque também não pode demorar demais, ou o proprietário e o fabricante questionarão a demora para a chegada do HSM no destino.

A substituição do HSM é mais rápida, pois o adversário só deve trocar o HSM enviado pelo fabricante por um HSM falso. O HSM falso será idêntico e possuirá as mesmas funções do original, porém com menos proteções físicas e lógicas, para facilitar o ataque em etapa posterior.

4.6.3 Recursos necessários

O acesso físico ao HSM geralmente é um dos requisitos para o ataque, mas neste caso o adversário já possui acesso físico. Para o envio de um HSM para seu proprietário, a entrega do dispositivo para a transportadora é o procedimento padrão, portanto a transportadora possui acesso físico ao HSM.

A modificação do HSM sendo transportado requer que o adversário conheça o dispositivo para que a modificação não seja detectada. A modificação não pode disparar sensores de intrusão física ou deixar vestígios no software, pois o proprietário não aceitará o HSM se ele notar que foi violado.

Para modificar o HSM, o adversário deve possuir ou conhecer o projeto do HSM para que ele possa modificar o dispositivo de forma sutil. Mesmo com conhecimento do HSM, um dispositivo homologado necessita de um ataque especializado para que seja atacado sem disparar sensores de intrusão física. Para modificar componentes do HSM é necessário possuir um laboratório especializado para executar o ataque.

A substituição do HSM é mais simples no sentido de que o dispositivo não precisa ser violado, nem mesmo o acesso físico é necessário se

a logística do ataque for bem coordenada. Para substituir, o adversário precisa conhecer como é a interface do HSM com o operador.

A substituição de um HSM não significa que o dispositivo malicioso possui as proteções do dispositivo original, significa que a sua interface com o operador é a mesma e a aparência física é a mesma. Se a interface com o operador for igual entre HSM malicioso e original, o operador não notará que o HSM foi substituído e o ataque pode ser executado posteriormente, quando o HSM estiver em uma etapa de gerenciamento de chaves.

4.6.4 Tempo necessário

A modificação de um HSM dura de horas a meses, pois o adversário pode possuir um laboratório preparado e conhecimento do funcionamento do HSM. Com conhecimento do HSM, a modificação do dispositivo é o tempo necessário para o ataque. Se o laboratório não foi preparado e o projeto não foi estudado para verificar como o ataque será realizado, o ataque pode levar meses.

A substituição do HSM significa que o dispositivo original simplesmente será substituído pelo malicioso que pode estar preparado. A substituição é um ataque que já foi preparado, portanto pode ser realizado em questão de segundos.

4.6.5 Trilha de auditoria

A transportadora não é uma entidade confiável para proteção do HSM, portanto dados de auditoria provenientes da transportadora não podem ser utilizados para rastrear o que houve com o dispositivo. Os únicos rastros de atividades relacionadas ao HSM que podem ser utilizados são provenientes do fabricante no momento do envio e do proprietário no momento do recebimento do HSM.

Os auditores conhecem as características externas de um HSM e seu modo de funcionamento. O conhecimento do auditor de como o HSM deve se parecer e se comportar deve ser utilizado para validar que o HSM é o mesmo que o fabricante enviou.

4.7 INSTALAÇÃO

A instalação do HSM é a etapa que inicia após o transporte do HSM. A instalação efetiva do HSM geralmente não inicia no momento exato em que o HSM é entregue ao proprietário, pois a instalação envolve uma cerimônia que envolve várias pessoas e a preparação da cerimônia leva algum tempo.

A etapa de instalação possui esse espaço de tempo ocioso entre a chegada do HSM nas mãos do proprietário e o início da cerimônia de instalação. Nesse espaço de tempo e em qualquer outro momento da etapa de instalação em diante, o HSM permanece em um ambiente com controle de acesso e monitoramento.

A cerimônia de instalação do HSM é o momento em que se define no equipamento quem serão os administradores, auditores e operadores do HSM. Outras configurações do HSM também são escolhidas nessa cerimônia, como o modo de operação do HSM.

4.7.1 Duração da etapa

A etapa de instalação do HSM dura de dez minutos a uma hora. A duração do tempo ocioso entre a chegada do HSM e o início da cerimônia de instalação é desconsiderado no cálculo de duração da etapa.

4.7.2 Ganho do adversário

O adversário tentará atacar o processo de instalação do HSM nesta etapa, ou seja, a cerimônia de criação de grupos do HSM. O adversário tentará ser inserido em um dos grupos do HSM.

Um adversário que obtém poder de um dos grupos poderá criar outros grupos ou criar chaves criptográficas, dependendo do grupo que ele utilizou como alvo do ataque. Outra função que o adversário poderá utilizar é a exportação de cópias de segurança (backup). As cópias de segurança contém as chaves criptográficas do HSM, mas de forma cifrada. É muito mais fácil obter as chaves explorando as cópias de segurança, pois o adversário não precisará burlar as proteções físicas do HSM.

O grupo que o adversário ataca é indiferente, pois se o atacante pode atacar um grupo, ele possui a capacidade de atacar qualquer grupo.

Outro tipo de ataque é a exploração de falhas no processo de autenticação. Em HSMs que utilizam smartcards como um dos fatores de autenticação, os smartcards podem ser trocados por cartões maliciosos, que são passíveis de clonagem ou extração de dados. Dessa forma, o adversário pode clonar os cartões e executar operações no HSM utilizando as permissões de outra pessoa.

4.7.3 Recursos necessários

Os grupos do HSM são definidos antes do início da cerimônia de instalação. O adversário deve fazer parte de um dos grupos para que o ataque seja possível sem a utilização de falhas criptográficas ou de hardware.

O adversário que usará falhas no processo de autenticação necessitam de acesso físico aos smartcards. Depois da criação dos grupos, o adversário deve acessar os smartcards e obter os dados dos cartões, seja via clonagem ou extração dos dados.

Seja qual for a forma de ataque, o adversário precisa de acesso físico ao HSM, para que possa executar as operações que ele conseguiu autorização com o ataque.

4.7.4 Tempo necessário

O adversário que é membro de um dos grupos do HSM, precisará de alguns minutos para executar o ataque.

O adversário substituindo smartcards por cartões maliciosos, precisará de semanas para testar o ataque no HSM alvo, antes de colocar o ataque em prática. A substituição de cartões e clonagem dura alguns minutos. A utilização dos cartões no HSM também levará alguns minutos.

4.7.5 Trilha de auditoria

O HSM irá registrar todas as operações executadas. No final da cerimônia de instalação, os auditores devem verificar se os logs do HSM são compatíveis com o registro da cerimônia. Qualquer incompatibilidade pode invalidar a cerimônia de instalação.

A detecção de smartcards defeituosos ou maliciosos não é algo que os auditores podem verificar com log seguro. Os membros dos gru-

pos do HSM devem proteger seus smartcards de acesso não autorizado. A proteção dos smartcards pode ser alcançada com políticas criadas pelos proprietários do HSM, guardando os cartões em um cofre sob vigilância e controle de acesso.

A utilização de cartões defeituosos para autenticação em HSMs é um tema que será discutido no capítulo 5, onde é realizada uma análise crítica das normas de homologação de HSMs.

4.8 GERAÇÃO DE CHAVES

A etapa de geração de chaves é o momento em que são criadas as chaves criptográficas que serão protegidas pelo HSM. A principal função do HSM é a proteção das chaves, portanto o material a ser protegido será gerado nesta etapa.

A cerimônia de instalação do HSM pode incluir a geração de chaves. Alguns proprietários podem incluir a geração de chaves no procedimento de instalação por questão de praticidade, pois os membros dos grupos estão presentes na cerimônia de instalação. Como a união da instalação do HSM e geração de chaves não é obrigatória, este trabalho separa os procedimentos em duas etapas.

4.8.1 Duração da etapa

A etapa de geração de chaves consiste em autenticar os administradores, gerar um ou mais pares de chaves criptográficas e atribuir um grupo de operadores como responsável de cada par de chave.

A duração desta etapa está diretamente ligada ao número de administradores que são necessários para autenticar o grupo, quantas chaves serão criadas e qual o tamanho das chaves criptográficas.

Cada administrador leva cerca de um minuto para se autenticar. Uma chave de até 2048 bits tipicamente leva poucos segundos para ser gerada no HSM. O processo ao todo dura cerca de 5 minutos.

4.8.2 Ganho do adversário

Como a única operação realizada nesta etapa é a geração de chaves criptográficas, o adversário interferirá na geração.

Chaves criptográficas são geradas a partir de bits aleatórios e a aleatoriedade dos bits é provida pelo gerador de números aleatórios

(RNG). O adversário pode induzir o RNG a criar dados que não são mais aleatórios. Um HSM que cria dados aleatórios previsíveis (bits com tendência maior de ser 0 ou 1) acaba gerando chaves criptográficas mais fáceis de serem quebradas com técnicas de criptoanálise.

4.8.3 Recursos necessários

Como a etapa de instalação do HSM já foi concluída, o proprietário considera que o HSM está em utilização ou produção. Um HSM em produção está sob vigilância e controle de acesso. O adversário deve conseguir acesso físico com o equipamento para atacar o HSM.

O adversário necessita de acesso físico ao HSM no momento em que for preparar o ataque. Este momento deve ser antes da geração da chave criptográfica. A preparação será facilitada se ela acontecer antes do início da cerimônia, pois será mais fácil encobrir o ataque, que precisa ser feito de forma que não seja detectado no momento da preparação ou após a preparação.

O ataque ao RNG pode ser via fonte de alimentação do HSM, alterando a corrente elétrica no momento da geração da chave criptográfica.

4.8.4 Tempo necessário

O tempo necessário para o ataque depende da tecnologia que o adversário tem a sua disposição. No melhor caso para o adversário, ele levará alguns minutos para preparar o ataque e no pior caso para o adversário, ele levará horas. Neste caso, a sua ocorrência durante a cerimônia de geração de chaves criptográficas será inviabilizada, pois o processo dura cerca de 10 minutos.

4.8.5 Trilha de auditoria

Nem sempre é possível obter a presença dos auditores durante esta etapa para verificar se houve a ocorrência de violação do HSM. Outra forma de verificação dos algoritmos deve ser executada.

A execução dos testes dos algoritmos do HSM antes da geração de chaves é suficiente para atestar que os algoritmos estão funcionando como deveriam. Os testes devem ser registrados no log do HSM que será exportado ao fim da operação.

Além da exportação dos logs do HSM no fim da operação é necessário exportar logs no início da etapa. Após a cerimônia os auditores devem obter a ata da cerimônia e qualquer registro de operações ocorridas.

Com os logs de operação do HSM extraídos antes e depois da cerimônia e a ata da cerimônia, os auditores podem verificar se algo errado aconteceu e se os testes dos algoritmos foram efetuados antes da geração de chaves. Se algo errado aconteceu, os auditores podem cancelar toda a cerimônia.

4.9 UTILIZAÇÃO DE CHAVES

Nesta etapa as chaves criptográficas são utilizadas. A utilização de chaves criptográficas consiste na utilização de algoritmos criptográficos onde uma das entradas do algoritmo é a chave criptográfica.

4.9.1 Duração da etapa

O tempo necessário para se utilizar uma chave criptográfica está relacionado com o número de operadores necessários para autenticar a utilização. O tempo necessário para assinar um dado também está relacionado, mas tipicamente este tempo é pequeno.

Em um exemplo, uma Autoridade Certificadora (AC) precisa assinar uma Lista de Certificados Revogados (LCR). Os operadores se autenticarão para carregar a chave para uma assinatura. Uma aplicação conectada ao HSM enviará um comando ao HSM, requisitando a assinatura do HASH da LCR. Todo este processo dura menos de 5 minutos.

No exemplo acima, desconsideramos o tempo necessário para que a aplicação que requer a assinatura execute suas operações internas.

4.9.2 Ganho do adversário

Nesta etapa o adversário pode explorar o carregamento da chave, para que seja executado de forma incorreta. As políticas do proprietário do HSM indicam que uma chave deve ser carregada para ser utilizada somente o número de vezes necessário. É também indicado que no fim do processo se verifique o estado da chave, para garantir que não pode mais ser utilizada.

O adversário pode persuadir os operadores para que carreguem a chave um número de vezes maior que o necessário para a operação. Por exemplo, carregar a chave para dez usos e utilizá-la apenas uma vez para assinar uma LCR. Desta forma o adversário pode utilizar a chave outras nove vezes da forma que desejar.

Outra forma é carregar a chave para infinitos usos e não descarregar a chave no fim do processo, desta forma o adversário poderá utilizar a chave para quantas assinaturas desejar.

É importante notar que a assinatura que os operadores necessitam realizar acontecerá normalmente, mesmo com a realização do ataque. Isso mostra que o ataque é bastante sutil e pode ser executado facilmente se os cuidados necessários não forem tomados.

4.9.3 Recursos necessários

Em uma cerimônia de utilização de chaves, existe uma pessoa que irá operar o computador e o HSM. O adversário deve ser esta pessoa que está operando o computador no momento da cerimônia ou ter alguma influência sobre a pessoa que está operando.

Uma cerimônia possui um roteiro que é seguido. O adversário pode alterar o roteiro da cerimônia, removendo ou incluindo ações que lhe convém para possibilitar o ataque.

4.9.4 Tempo necessário

O ataque é realizado com a alteração de um parâmetro (número de usos da chave), portanto ele pode ser realizado em segundos.

4.9.5 Trilha de auditoria

A cerimônia segue um roteiro que está de acordo com as políticas estabelecidas pelo proprietário do HSM. Os auditores devem coletar o roteiro da cerimônia, o registro de operações ocorridas durante a cerimônia, os logs do HSM no início e fim da utilização de chaves.

Com a coleta das várias informações, os auditores podem verificar se o roteiro e o registro da cerimônia estão de acordo com as políticas do proprietário, e se as operações realizadas no HSM estão de acordo com o que foi definido na cerimônia.

4.10 AUDITORIAS PERIÓDICAS

Um adversário pode tentar utilizar chaves criptográficas ou acessar o HSM indevidamente em qualquer momento do ciclo de vida do HSM. As auditorias periódicas existem para verificar se o HSM foi violado após a sua instalação.

A auditoria periódica consiste em resgatar os logs de operação do HSM e verificar se ocorreu a sua utilização incorreta. A frequência com que as auditorias ocorrem é definida pelo proprietário do HSM e a frequência depende de vários fatores como importância das chaves, número de acessos ao HSM e nível de proteção física do ambiente em que o HSM está.

A importância da chave está ligada ao impacto monetário ou estratégico da chave armazenada no HSM. Se o impacto do comprometimento da chave for grande, auditorias mais frequentes são necessárias.

O número de acessos ao HSM dá ao adversário mais espaço para executar o ataque, principalmente se o adversário é uma das pessoas que acessa o HSM. Quanto maior o número de acessos, menor deve ser a frequência de auditorias.

O ambiente do HSM pode facilitar ou dificultar muito a ação do adversário, sendo que ambientes com controle de acesso e monitoramento rigoroso podem inviabilizar vários ataques de caráter físico. Ambientes com proteção física e controle de acesso fraco necessitam de auditorias mais frequentes.

A etapa de auditoria periódica é executada apenas pelos auditores. Os auditores extrairão os logs do HSM para verificar se houve a utilização indevida do dispositivo. Os auditores checarão a integridade física do HSM. Um adversário pode atacar as proteções físicas do HSM e deixar rastros visíveis, que são fáceis de visualizar com o rompimento de selos de evidenciação de abertura, comuns em HSMs. Os auditores procurarão estes rastros para verificar se houve uma tentativa de violação.

4.10.1 Duração da etapa

Os auditores extrairão os logs do HSM e a duração da etapa está diretamente ligada ao tamanho do arquivo de log.

O processo de extração dos logs do HSM e verificação de violação física tipicamente dura menos de 10 minutos.

4.10.2 Ganho do adversário

Na etapa de auditoria periódica o adversário tentará causar a negação de serviço (DoS) no HSM. Se o adversário conseguir provar para os auditores que o HSM foi violado ou que sua utilização indevida ocorreu, o HSM não pode mais ser utilizado causando assim a negação do serviço criptográfico provido por esse dispositivo.

O adversário pode provocar a violação física do HSM, ou convencer os auditores de que a violação física ocorreu. Outra forma é convencer os auditores de que a chave foi utilizada inadequadamente, forjando os logs extraídos do HSM ou substituindo estes logs por outros previamente preparados.

O procedimento a ser adotado pelos auditores ao verificar que uma tentativa de invasão ocorreu ou que as chaves foram utilizadas de forma incorreta, é bloquear o HSM para que todo o seu conteúdo seja excluído e as chaves armazenadas não possam mais ser utilizadas. Em uma ICP por exemplo, o bloqueio de um HSM pode significar o comprometimento de todo um ramo da ICP.

4.10.3 Recursos necessários

É necessário acesso físico ao HSM para disparar um dos sensores de intrusão física, ou para violar os selos de evidenciação de abertura.

Para forjar os logs do HSM, indicando que a sua utilização inadequada ocorreu, é necessário conhecimento de como o HSM funciona para que os logs sejam forjados de forma convincente. É possível que os logs sejam assinados, dificultando o processo de substituição ou modificação destes logs.

4.10.4 Tempo necessário

O tempo necessário para ativar um sensor físico é menor do que 5 minutos. Para forjar um arquivo de log é necessário mais tempo, pois se o adversário não souber como irá forjar ou substituir o arquivo de log ele deverá estudar o ataque antes.

4.10.5 Trilha de auditoria

A etapa de auditoria periódica é realizada pelos próprios auditores, portanto não é necessário que os auditores avaliem e aprovem suas próprias ações. Mecanismos que auxiliarão no processo de auditoria é a assinatura dos logs do HSM, para garantir que não foram forjados. A assinatura dos logs prova a sua autenticidade, ou seja, significa que foram gerados pelo HSM a pedido dos auditores.

Os auditores não devem aceitar um arquivo de log do HSM que não foi assinado, ou com assinatura inválida.

4.11 DESCARTE

O proprietário de um HSM pode se desfazer do equipamento a qualquer momento. Se desfazer de um HSM pode resultar em várias situações diferentes: a destruição do HSM, exclusão do seu conteúdo para revendê-lo ou simplesmente guardar o HSM.

A etapa de descarte do HSM é a última etapa do ciclo de vida do dispositivo. O descarte do HSM com a sua destruição acontece de forma um pouco mais simples que o descarte sem destruir o dispositivo. A destruição do HSM deverá acontecer respeitando a política de destruição estipulada pelo proprietário. A destruição de um HSM consiste em moer o HSM várias vezes ou incinerar o dispositivo para garantir que os fragmentos do HSM não podem ser utilizados para remontar o segredo.

A venda do HSM se encaixa num cenário onde o dispositivo será descartado sem a destruição. Nessa situação, as chaves criptográficas e todo o material secreto do HSM devem ser excluídos antes que o HSM possa ser considerado pronto para ser repassado. Se uma chave criptográfica for carregada na memória RAM por um longo período, é possível que o valor da chave fique gravado na memória, mesmo após a exclusão.

O repasse de um HSM deve ser realizado com maior cuidado que a destruição, sendo necessário descarregar qualquer forma de corrente elétrica armazenada na eletrônica do HSM, para que as chaves sejam descarregadas por completo.

O fim do ciclo de vida de uma chave criptográfica é a sua destruição. Este trabalho não trata do ciclo de vida de chaves criptográficas e sim do ciclo de vida de módulos de segurança criptográfica, portanto o descarte de um HSM não significa a destruição de uma chave cripto-

gráfica, pois podem existir cópias de segurança desta chave. O ciclo de vida de chave criptográficas é tratado no trabalho (MARTINA; SOUZA; CUSTODIO, 2007).

4.11.1 Duração da etapa

Para garantir que o HSM foi descartado sem manter dados sigilosos o tempo necessário é de dias a semanas.

4.11.2 Ganho do adversário

Um HSM que teve seu conteúdo de chaves excluído, pode possuir chaves gravadas em memória volátil. O adversário pode utilizar técnicas para resgatar esta chave da memória RAM do HSM, mesmo após o descarte do dispositivo. Com isso o adversário pode ter acesso ao material de chave.

A destruição de um HSM deve ser realizada de forma que os pedaços restantes do dispositivo possam ser utilizados para resgatar dados do HSM. O adversário tentará obter o que restou do HSM após a destruição e resgatar as chaves criptográficas que eram gerenciadas pelo dispositivo.

Os problemas relacionados a chaves criptográficas em memória persistente não são tratados neste trabalho. Chaves criptográficas em disco são protegidas por criptografia e isto é um requisito das normas de homologação, portanto apenas problemas relacionados a chave em memória volátil são tratados.

4.11.3 Recursos necessários

O adversário deve obter acesso físico ao HSM após o descarte. O adversário pode ser a pessoa que comprou o HSM após o descarte, ou pode conseguir os pedaços do HSM em caso de destruição do dispositivo.

É necessário que o adversário possa utilizar um laboratório especializado para a recuperação dos dados da memória em caso de um HSM funcional, ou obtenção de dados a partir de um HSM destruído.

4.11.4 Tempo necessário

O tempo necessário para recuperar dados de um HSM descartado é de dias a semanas. Este tempo é necessário para resgatar dados tanto de um HSM descartado, quanto de um HSM destruído. A análise dos dados resgatados para identificar quais dados são relevantes (chaves criptográficas) também interfere no tempo necessário.

4.11.5 Trilha de auditoria

Os auditores devem extrair os logs do HSM antes do descarte, para verificar se a utilização indevida do equipamento ocorreu no período entre a última auditoria e o momento do descarte.

O ataque de recuperação de dados da memória RAM de um HSM descartado pode ser amenizado sobrescrevendo toda a memória RAM antes do descarte do HSM. O dispositivo pode possuir uma função que apaga todas as informações do HSM, e nesta operação a memória pode ser sobrescrita.

As normas de homologação possuem como requisito a sobrescrita do local de memória que armazenou chaves em claro, com bits aleatórios, processo conhecido como "zeramento" da memória. A sobrescrita apenas das chaves criptográficas não impede o resgate de outros dados críticos que não são chaves criptográficas.

Para dificultar a recuperação de dados de um HSM destruído, é necessário aplicar técnicas diferenciadas de destruição de dispositivos. Técnicas como dissolver a eletrônica do equipamento ou moer o HSM em pedaços extremamente pequenos, dificultarão o resgate de dados após a destruição.

4.12 CONCLUSÃO

Este capítulo descreve vulnerabilidades que podem existir em HSMs, com o intuito de criar um processo de auditoria capaz de detectar ataques utilizando estas e outras vulnerabilidades durante cada etapa do ciclo de vida.

Este capítulo além de descrever quais são as etapas do ciclo de vida, descreve quais são os rastros gerados em cada etapa. A proposta deste trabalho utiliza esses rastros como a base da unificação da auditoria.

O processo de unificação é descrito no capítulo 5, e nesse processo os rastros de auditoria de uma etapa podem ser utilizados nas etapas posteriores, com o intuito de auditar ou comprovar que o HSM não foi comprometido. Com os rastros de auditoria é possível descobrir o que ocorreu com o HSM, se um ataque for detectado ou houver a suspeita de ataque ao HSM.

O capítulo 6 deste trabalho propõe a adaptação das normas de homologação, para que incluam requisitos que possibilitem a auditoria unificada em HSMs homologados. A alteração das normas é baseada na adição de funcionalidades em HSMs, para que esses dispositivos gerem rastros de auditoria.

Com as contribuições deste capítulo podemos notar que a proposta e as alterações nas normas não modificam apenas o processo de montagem de HSMs, mas também modifica o comportamento do fabricante. O fabricante deve demonstrar cuidado na etapa de concepção do HSM, com o controle de versão do software do HSM e controle de acesso na etapa de fabricação, por exemplo.

5 UNIFICANDO A AUDITORIA DE HSMS

5.1 INTRODUÇÃO

A literatura não descreve como realizar a auditoria unificada de todas as etapas do ciclo de vida do HSM. Para cada etapa existem técnicas apropriadas de auditoria para validar a sua segurança.

Este capítulo apresenta uma forma de unificação das etapas do ciclo de vida, para garantir que o HSM projetado tenha sido submetido a todos os processos de auditoria e que seja, após o término de sua vida útil, descartado com segurança.

O processo de unificação se baseia na propagação da auditoria em uma etapa do HSM, para as etapas posteriores. Em algums casos não é possível a propagação dos rastros de auditoria, portanto é necessário validar a etapa de alguma forma. Esse é o caso das etapas de projeto e amostra de engenharia, que são validadas pela etapa de homologação e apresentadas neste capítulo.

Para o melhor entendimento do leitor, a unificação da auditoria do ciclo de vida foi dividida em dois períodos, pré-instalação e pós-instalação. A divisão é apresentada na figura 4.

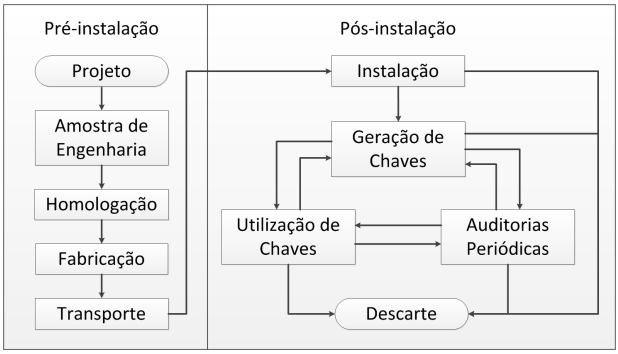

Figura 4: Seções de pré-instalação e pós-instalação

O período de pré-instalação é o momento em que o proprietário do HSM ainda não teve acesso ao dispositivo, ou seja, apenas o fabricante, órgão de homologação e transportadora manusearam o dispositivo. No período de pós-instalação, é necessário que o HSM possua

algumas funções específicas para que a auditoria possa ser realizada.

É necessário que os fabricantes produzam HSMs que permitam a auditoria em todo o ciclo de vida. O proprietário de um HSM não poderá extrair logs de operação, por exemplo, se o HSM não possui essa funcionalidade.

Para garantir que os HSMs possuirão funcionalidades de auditoria, é necessário incluir requisitos nas normas de homologação que forcem os fabricantes a incluir estas funcionalidades.

Homologação: O processo de homologação é executado pelo órgão de homologação, e atesta que um HSM está em conformidade com uma norma que contém uma série de requisitos de segurança, funcionalidade e documentação.

O capítulo 6 sugere alterações nas normas para incluir requisitos relacionados a auditoria de HSMs em qualquer etapa do ciclo de vida do dispositivo.

A seção 5.2 apresenta o período de pré-instalação e a seção 5.3 apresenta o período de pós-instalação.

5.2 PRÉ-INSTALAÇÃO

O período de pré-instalação é uma parte do ciclo de vida do HSM que inicia no projeto criado pelo fabricante e termina quando o HSM é entregue ao proprietário, ou seja, assim que termina o transporte do HSM. Todas as etapas da seção de pré-instalação ocorrem antes do evento de instalação do HSM.

Seria ideal se a auditoria dos HSMs pudesse ser realizada pelos auditores em todas as etapas do ciclo de vida, porém isso nem sempre é possível. O mais comum é a situação onde os auditores só tem acesso ao HSM depois que o transporte é realizado, portanto os rastros de auditoria gerados na seção de pré-instalação devem ser tratados por outras pessoas ou entidades.

Rastro de auditoria: Informações e artefatos que são coletados durante o ciclo de vida de um HSM para verificar o que ocorreu com o HSM. Os artefatos de auditoria que compõem os rastros de auditoria podem ser os logs de operação do HSM, por exemplo.

Para que os rastros da pré-instalação possam ser utilizados pelos auditores, esses devem ser gerados ou avaliados por entidades em que

os auditores confiam. Num cenário de ICP, por exemplo, os auditores confiam apenas no órgão de homologação, que avalia os rastros de auditoria.

O órgão de homologação deve analisar o HSM e verificar se o fabricante pode ser confiado para produzir o HSM em questão. Desta forma, uma cadeia de confiança é criada, onde os auditores confiam no HSM, pois foi montado pelo fabricante que é de confiança do órgão de homologação. A relação de confiança entre fabricante e órgão de homologação é estabelecida no processo de homologação do HSM.

5.2.1 Validação do projeto

O ciclo de vida do HSM se inicia no projeto do dispositivo. O único ponto de confiança dos auditores neste momento é o órgão de homologação. No momento do desenho do projeto, não há como se homologar o HSM da forma como os órgãos de homologação trabalham hoje, pois da forma atual se homologa um HSM pronto para gerenciar chaves.

Na etapa de projeto o fabricante deve manter a trilha de auditoria, que é o registro de modificações no projeto.

Após o projeto do HSM o fabricante produz algumas amostras do HSM, as amostras de engenharia. A trilha de auditoria das amostras indica com detalhes quem foram as pessoas que participaram e tiveram acesso às amostras de engenharia durante a sua montagem.

O próximo passo é a homologação do HSM. Neste trabalho propõe-se que os rastros de auditoria das etapas de projeto e amostra de engenharia sejam entregues ao órgão de homologação. Os rastros devem ser entregues pois é inviável para o órgão de homologação participar do processo de montagem das amostras de engenharia. Se os processos de homologação iniciassem a partir da concepção de um HSM, seria possível para o órgão homologador verificar se a amostra foi produzida de forma segura.

Premissa: Os auditores e fabricantes confiam no órgão de homologação. Os fabricantes confiam que a documentação, projeto e código-fonte enviados ao órgão de homologação não serão divulgados. Os auditores confiam no atestado de conformidade emitido pelo órgão de homologação.

Com algumas amostras de engenharia montadas o fabricante envia equipamentos para o órgão de homologação, com o intuito de re-

ceber a certificação do equipamento. Esta é a etapa de homologação do HSM, uma das etapas do ciclo de vida. Se o órgão de homologação atestar que o HSM está em conformidade com os requisitos da norma, é concluída a unificação das três primeiras etapas do ciclo de vida: projeto, amostra de engenharia e homologação.

O órgão de homologação além de suas atividades normais, irá verificar se houve a preocupação por parte do fabricante em armazenar a trilha de auditoria das etapas de projeto e amostra de engenharia. Se houve a preocupação, o órgão de homologação pode atestar que o fabricante realizou a auditoria do HSM nas primeiras etapas do ciclo de vida.

A auditoria das primeiras etapas junto com a homologação do equipamento, tornam o fabricante do HSM uma entidade confiável para a fabricação do dispositivo específico.

A trilha de auditoria também deve ser criada para a etapa de homologação. A trilha de auditoria criada na etapa de homologação é composta pelo registro detalhado de atividades durante a homologação do HSM.

Requisitos para criação da trilha de auditoria na etapa homologação não são necessários, pois o órgão de homologação já é uma entidade confiável. Por padrão considera-se que o órgão homologador gera e armazena a trilha de auditoria da homologação.

5.2.2 Fabricação e transporte

As etapas de fabricação e transporte estão em um espaço intermediário entre as etapas que envolvem os auditores e o órgão de homologação. Estas duas etapas são conduzidas na maior parte do tempo pelos fabricantes de HSMs.

Como a etapa de fabricação é posterior à de homologação, significa que existe um certo nível de confiança no fabricante dos HSMs.

O fabricante, como entidade confiável no processo, assume responsabilidade sobre as questões de segurança do processo de montagem dos HSMs. As questões de segurança são o controle de acesso ao local de montagem dos HSMs e monitoramento das atividades da equipe que monta os HSMs.

Conforme descrito na seção 4.5, a utilização de Hardware Trojans na fabricação de HSMs é um problema que pode afetar todo um lote de dispositivos se o fabricante não adquirir os componentes corretos. Uma forma de conscientizar o fabricante da importância de utilizar

o componente correto, é incluir como requisito nas normas de homologação a indicação da marca e modelo de cada componente que será utilizado no HSM.

A descrição de todos os componentes de hardware utilizados no HSM indica que só dispositivos com aqueles componentes foram homologados. Se houver a detecção de um HSM que utiliza um componente de hardware fora dos listados, este HSM não pode ser considerado um dispositivo homologado.

Após a fabricação do HSM, inicia a etapa de transporte. Essa etapa também é responsabilidade do fabricante do HSM.

Um HSM recém montado pode ser armazenado para posteriormente ser enviado ao proprietário, ou idealmente o HSM sai da montagem e já é enviado para o proprietário. O primeiro caso é mais comum, pois geralmente o lote de HSMs é vendido e os dispositivos são enviados após um certo tempo.

O transporte é uma etapa difícil de ser monitorada, pois geralmente nesta etapa o HSM fica fora das mãos das três entidades confiáveis, o órgão de homologação, cliente (ou futuro proprietário) e fabricante do HSM.

Existem poucas formas de proteger um HSM contra substituição completa do dispositivo ou modificação não autorizada de componentes. Não só é difícil proteger o HSM contra violação, como também é difícil obter uma trilha de auditoria do que ocorreu com o dispositivo durante o transporte.

Um HSM por definição é um dispositivo criptográfico capaz de no mínimo evidenciar se ocorreu uma tentativa de violação. Portanto, um ataque físico durante a etapa de transporte deveria ser detectado pelos auditores. No entanto, a substituição completa de um HSM não deixará evidências de violação.

A substituição completa de um HSM homologado é algo que pode ser evitado com uma solução criptográfica, utilizando a premissa de que um ataque físico será evidenciado pelos auditores.

No momento que um HSM na linha de produção tem seu ciclo de montagem completo, esse HSM irá gerar uma chave. A chave gerada pelo HSM se chama chave de inicialização e será exportada de forma que apenas o fabricante a conheça. Isso pode ser feito por exemplo, através de um texto, token criptográfico, cartão de memória, mídia digital ou até mesmo impressa. A chave de inicialização será entregue por um canal seguro para o proprietário do HSM, ou para seus auditores.

Na primeira inicialização do HSM, a chave de inicialização deve ser utilizada para validar a inicialização. Se o HSM detectar um ata-

que durante o transporte, a chave de inicialização que ele possui será apagada e sobrescrita. Um HSM que substitui o original, não possui a chave de inicialização e não pode ser considerado como um HSM que foi enviado pelo fabricante.

Desta forma a auditoria nas etapas de homologação, fabricação, transporte e inicialização são unidas no ciclo de vida do HSM.

5.3 PÓS-INSTALAÇÃO

O período de pós-instalação é a parte do ciclo de vida do HSM que complementa a pré-instalação. A pós-instalação inicia na etapa de instalação do HSM e termina quando o HSM é descartado.

Esta seção apresenta um marco para a unificação dos ciclos de vida de HSMs, pois o dispositivo já foi entregue ao seu proprietário e portanto os auditores tem acesso ao HSM. No período de pré-instalação a trilha de auditoria do HSM e sua segurança eram atribuídas ao fabricante e ao órgão de homologação. No período de pós-instalação são os auditores que verificam se o HSM está sendo utilizado de forma apropriada.

5.3.1 Instalação

A etapa de instalação de um HSM é a primeira da pós-instalação, onde ocorre a sua inicialização.

O processo descrito na seção 5.2.2 define o que é a inicialização segura do HSM utilizando a chave de inicialização gerada na fabricação do HSM. Antes que qualquer operação possa ser realizada no HSM, a inicialização segura deve ocorrer. O proprietário do HSM ou os auditores devem inicializar o dispositivo.

É necessário que o proprietário do HSM ou os auditores verifiquem se houve a tentativa de violação física do HSM durante o transporte.

Os auditores ou o proprietário do HSM podem considerar a seção de pré-instalação válida nas seguintes condições:

- O HSM foi homologado;
- Nenhuma tentativa de violação foi detectada;
- O HSM foi inicializado com a chave de inicialização.

Após a inicialização segura, o HSM está apto para geração dos grupos que administrarão as suas operações, como os auditores e operadores de chaves criptográficas.

A configuração desses grupos do HSM é definida nas políticas de utilização do dispositivo, que são criadas pelo proprietário do HSM. As políticas de utilização são uma série de regras que definem como o HSM deve ser configurado e utilizado.

A criação dos grupos do HSM é um procedimento que segue uma cerimônia. Os passos da cerimônia devem respeitar as políticas de utilização. Antes da execução da cerimônia, os auditores devem verificar se os passos estão de acordo com as políticas de utilização do HSM.

A execução da cerimônia deve ser documentada no log da cerimônia. Este log contém todos os passos da cerimônia em detalhe, indicando qualquer erro que ocorra no procedimento ou acontecimento fora do esperado.

Os auditores devem verificar se o HSM possui alguma configuração antes do início da cerimônia de criação dos grupos, pois qualquer configuração existente pode comprometer a segurança do HSM.

Os auditores devem obter uma cópia do log da cerimônia após a sua realização e verificar se o log condiz com o roteiro e se nenhuma irregularidade ocorreu.

Na ocorrência de qualquer irregularidade os auditores poderão relatá-las, indicando que o HSM não pode ser utilizado com segurança.

Após a instalação do HSM, é possível ir para uma de três etapas: geração de chaves, auditorias periódicas ou descarte.

5.3.2 Geração de chaves

A geração de chaves criptográficas no HSM é uma das principais etapas do ciclo de vida de um HSM. Cada chave gerada deve ser associada a um grupo de custodiantes. Conforme definido na seção 3.5.1, denominamos esse grupo de operadores.

Os grupos de um HSM são criados na etapa de instalação do dispositivo, portanto a etapa de geração de chaves deve ocorrer depois da instalação.

Esta etapa pode ser iniciada sempre que for necessário gerar uma nova chave criptográfica no HSM.

Com o objetivo de gerar o maior número de evidências possíveis para auditoria, a geração de chaves deve seguir uma sequência de ati-

vidades descritas em uma cerimônia previamente estabelecida. Como resultado, além da associação das chaves aos grupos de operadores, um relatório é emitido, onde todos os participantes da cerimônia o assinam.

Além do relatório, o registro de todas as operações internas ao HSM é feito em arquivos de log. Assim, os auditores podem fazer uso tanto do relatório da cerimônia, quanto dos logs para constatar se as atividades respeitam as políticas de utilização do HSM.

Após a geração de chaves é possível utilizá-las na etapa de utilização de chaves.

5.3.3 Utilização de chaves

A etapa de utilização de chaves é simples do ponto de vista de auditoria. Assim como na geração, a utilização das chaves acontece em uma cerimônia, que possuirá um roteiro e um log.

A trilha de auditoria da utilização de chaves é composta do roteiro da cerimônia, o log da cerimônia e o log de operações do HSM. Estes três componentes devem ser compatíveis entre si e estar de acordo com as políticas de utilização do HSM.

Cada uso da chave deve ser rastreado. Informações como quem e quando uma chave foi usada, devem estar presentes nos logs da cerimônia e do HSM.

5.3.4 Auditorias periódicas

Ataques a um HSM podem acontecer em todo o ciclo de vida do HSM, inclusive entre etapas. A etapa de auditorias periódicas existe para preencher esta lacuna e verificar a ocorrência de ataque nesses momentos.

Tomando como exemplo um HSM que é utilizado uma vez por mês, o intervalo de tempo em que o HSM não foi utilizado é suficiente para um ataque elaborado ao dispositivo.

A trilha de auditoria desta etapa consistem na exportação de logs do HSM, um procedimento que tipicamente leva menos de 10 minutos. Voltando ao nosso exemplo, é possível exportar esses logs uma vez por semana, ou mesmo diariamente, para dificultar a execução de um ataque ao HSM.

As auditorias periódicas do HSM acontecem com uma frequência de tempo definida na política de utilização do HSM.

5.3.5 Descarte

O descarte do HSM é a etapa em que o dispositivo sai de operação, ou seja, poderá ser destruído, armazenado, vendido ou repassado para outra entidade. Cuidados são necessários para garantir que o HSM não possua dados sigilosos em memória volátil e memória persistente no momento do descarte.

Aplicações que utilizam chaves criptográficas e dados sensíveis geralmente utilizam estes dados em memória volátil, já que o tempo de busca de dados em memória volátil é muito inferior ao tempo de busca em memória persistente. Entretanto, os dados devem ser guardados em memória persistente para que sejam preservados por um longo período de tempo.

As chaves em memória persistente devem ser protegidas por algoritmos de sigilo, ou seja, devem ser cifrados. Estas chaves podem ser decifradas e armazenadas em memória volátil pelo tempo necessário à sua utilização.

No descarte do HSM as chaves cifradas em memória persistente podem ser sobrescritas, e apesar de ser uma conduta recomendável, não é vital para a segurança das chaves no descarte do HSM. Ao contrário das chaves em memória persistente, é vital que as chaves em memória volátil sejam sobrescritas com zeros sempre que não forem mais necessárias, para evitar que sejam copiadas por um atacante.

A recomendação é que na etapa de descarte as chaves em memória persistente sejam sobrescritas com zeros e toda a memória volátil seja sobrescrita para evitar a busca e recuperação de chaves criptográficas.

Os logs de operação do HSM confirmam que as operações de limpeza das memórias foram executadas e estes logs devem ser exportados pelos auditores antes do seu descarte. Portanto deve haver uma maneira de ser exportar os logs mesmo após a limpeza das memórias, ou seja, a limpeza não pode excluir os logs de operação do HSM.

5.4 CONCLUSÃO

Este capítulo descreveu a unificação da auditoria no ciclo de vida de HSMs que é a proposta principal do trabalho. A proposta é dividida em dois períodos nas seções 5.2 e 5.3, conhecidos como pré-instalação e pós-instalação, respectivamente.

A contribuição deste capítulo é a apresentação das preocupações

e operações que devem ser executadas para que a trilha de auditoria seja gerada durante todo o ciclo de vida do HSM.

A unificação requer controle dos artefatos que envolvem a fabricação e operação do HSM, ou seja, de todo o ciclo de vida do HSM. Este capítulo descreveu que o projeto, amostra de engenharia e homologação requerem procedimentos específicos para evitar que um HSM defeituoso seja projetado.

Posteriormente foi apresentado que a fabricação do HSM requer controle dos componentes utilizados na montagem. Também foi apresentada a preocupação em criar um procedimento criptográfico para atestar que o HSM não foi atacado ou substituído durante o seu transporte.

Por fim, esse capítulo mostra que cerimônias são essenciais para a geração de artefatos de auditoria no HSM, que servem como forma de registro de atividades executadas no HSM.

O entendimento da unificação da auditoria apresentada nesse capítulo é necessário para entender o próximo capítulo, que descreve as alterações em normas de homologação. O capítulo 6 descreve o que deve ser alterado nas normas, para que seja possível gerar todos os artefatos de auditoria e executar todos os procedimentos descritos neste capítulo.

6 ALTERAÇÕES NAS NORMAS DE HOMOLOGAÇÃO

6.1 INTRODUÇÃO

Este capítulo propõe alterações nas normas de homologação de HSMs para que se possa realizar a auditoria unificada em qualquer HSM homologado, no contexto das normas FIPS 140-2 e MCT 7. As alterações nas normas de homologação visam transformar a trilha de auditoria das etapas do ciclo de vida do HSM em um requisito para a homologação.

A FIPS 140-2 estabelece níveis de segurança que definem a quantidade e qualidade das proteções do HSM. Esses níveis vão de 1 a 4, sendo 4 o nível com as melhores proteções para o conteúdo sensível do HSM. Já o MCT 7 possui dois tipos diferentes de homologação, o Nível de Segurança de Homologação (NSH) e o Nível de Segurança Física (NSF), cada um com vários níveis, sendo o NSH de 1 a 3 e o NSF de 1 a 2.

Pode-se incorporar os novos requisitos às normas de homologação, levando em conta a existência dos níveis de homologação atuais, de 3 formas distintas:

a) Adequação dos atuais níveis de homologação: a adequação consiste em atrelar os novos requisitos aos níveis de homologação existentes;

b) Inclusão de um nível adicional de homologação: esse novo nível faria com que a FIPS 140-2 possuísse mais um nível, assim a norma começaria com o nível 1 e iria até o nível 5. A norma MCT 7 receberia um nível no NSH, começando com o nível 1 e chegando ao nível 4. Esses novos níveis irão conter os requisitos relacionados a auditoria;

c) Inclusão de outro tipo de homologação: a inclusão de um tipo de nível faria com que a FIPS 140-2 se tornasse uma norna mais semelhante a MCT 7. Com a inclusão de um tipo de homologação, a FIPS 140-2 possuiria dois tipos de homologação: o primeiro tipo com níveis de 1 a 4; outro tipo que é relacionado com auditoria, com dois níveis. O MCT 7 possuiria os dois tipos de homologação que já existem, e terceiro, o Nível de Segurança de Auditoria (NSA), com os níveis 1 e 2.

A escolha da proposta de incorporação dos novos requisitos entre

as opções a), b) e c) deve levar em consideração o impacto das alterações nos HSMs que já foram homologados.

Também consideramos que os HSMs homologados só atendem os requisitos das normas atuais, ou seja, os HSMs homologados não atendem aos requisitos adicionados neste trabalho.

A proposta a) de incorporar os novos requisitos, adaptação dos níveis de homologação, mescla os requisitos novos com os requisitos já existentes. Os HSMs já homologados não atendem aos requisitos novos (requisitos de auditoria). Assim, os HSMs já homologados não serão compatíveis com a nova norma que possui níveis de homologação adaptados.

A proposta b) de incluir os novos requisitos aumenta os níveis de homologação existentes. Se o novo nível (de auditoria) for inserido como o nível máximo, os HSMs já homologados serão compatíveis. Se o nível de auditoria for inserido entre os níveis atuais, os HSMs já homologados não serão compatíveis, pois um HSM no nível máximo deve atender aos requisitos de todos os níveis da norma. Por exemplo, um HSM nível 5 deve atender aos requisitos dos níveis 1 ao 5. Se os requisitos de auditoria estiverem no nível 3, um HSM já homologado não será compatível, pois ele não atende aos requisitos de auditoria que estão no nível 3.

A proposta c) de adicionar requisitos inclui um novo tipo de nível de homologação ao processo. Todos os requisitos de auditoria seriam inseridos nesse novo tipo de nível de homologação. Os HSMs que já foram homologados serão compatíveis com a norma, pois os níveis de homologação aos quais eles foram homologados não foram modificados.

A proposta c) é a abordagem escolhida neste trabalho. O impacto da proposta c) é o menor das opções apresentadas, pois as alterações nas normas mantém a compatibilidade dos HSMs já homologados sob as normas sem alteração.

Outra vantagem da proposta c) é que esta deixa claro quais são as funções relacionadas com auditoria, na criação de um novo tipo de homologação, com os níveis de auditoria. A homologação de HSMs que seguem os requisitos de auditoria mostrará quais são os HSMs que possuem funções de auditoria e quais fabricantes se preocupam com a auditoria de seus equipamentos.

Com os requisitos de auditoria, as normas de homologação se tornarão ainda mais importantes em contextos onde a auditoria é essencial para a segurança do sistema, como em ICPs.

Uma ICP geralmente possui controles rígidos e requerem o maior número de proteções possível, portanto um HSM só poderá ser utilizado

em uma ICP se possuir homologação no nível máximo de auditoria. Em outro contexto, o proprietário de um HSM utilizado para gerência de chave e que não tem necessidade de realizar a checagem do estado do HSM, não necessita de funções de auditoria, portanto atribuirá importância menor aos níveis de auditoria.

As próximas seções apresentam quais requisitos devem estar contidos nos novos tipos de nível de homologação. Para as duas normas consideradas neste trabalho, o nível de auditoria será chamado Nível de Segurança de Auditoria (NSA).

A seção 6.2 apresenta as alterações nas normas que são relacionadas com as etapas do ciclo de vida de validação do projeto. A seção 6.3 segue apresentando as alterações relacionadas às etapas de fabricação e transporte, e o restante das etapas é reunido na seção 6.4, que apresenta as alterações nestas etapas do ciclo de vida.

6.2 VALIDAÇÃO DO PROJETO

As etapas do ciclo de vida do HSM que compõem a validação do projeto são: projeto, amostra de engenharia e homologação. Para o novo tipo de homologação que está sendo proposto, o NSA, as normas de homologação devem requerer que sejam depositados os artefatos necessários para montar a trilha de auditoria da validação de projeto.

Os artefatos são: a confirmação de que existiu um controle de versões no projeto do HSM; e a confirmação de que o fabricante se preocupou em manter as amostras de engenharia sob controle de acesso para dificultar a modificação não autorizada.

6.2.1 FIPS 140-2

A norma FIPS 140-2 possui uma seção dedicada para questões que envolvem o desenvolvimento do HSM a ser homologado, que é a seção 4.10.3. De forma geral essa seção indica que o fabricante deve enviar os esquemáticos do HSM e o código fonte do software contido no dispositivo.

A quantidade de artefatos a serem depositados depende do nível de segurança de homologação requisitado, e o depósito pode ir da simples entrega de código fonte até a representação formal de que o HSM cumpre a política de segurança apresentada.

A FIPS 140-2 não requisita que seja depositada uma trilha de

auditoria de validação do projeto. O novo tipo de homologação, o NSA da FIPS 140-2, deve requerer que o fabricante envie dados que comprovem a existência do controle de versões durante o desenvolvimento do HSM.

Além do controle de versão do projeto, é necessário comprovar que houve a preocupação em monitorar quem participou da montagem da amostra de engenharia, com detalhes como data, hora e o que foi modificado na amostra.

6.2.2 MCT 7

A seção 3.10 do MCT 7, assim como a seção 4.10.3 da FIPS 140-2, contém requisitos relacionados aos esquemáticos do HSM e código fonte do software do dispositivo.

Da mesma forma que a FIPS 140-2, faltam requisitos que auxiliam na formação da trilha de auditoria das etapas de validação do projeto. Devem ser incluídos mais dois requisitos, um relacionado ao depósito da trilha de auditoria da etapa de projeto e um segundo requisito relacionado à trilha de auditoria da etapa de amostra de engenharia.

Os dois requisitos podem ser incluídos na seção 3.10 e devem fazer parte do NSA do MCT 7.

6.3 FABRICAÇÃO E TRANSPORTE

Esta seção indica quais são as modificações necessárias às normas de homologação para requerer artefatos que comprovem a existência da trilha de auditoria das etapas de fabricação e transporte do HSM.

Os artefatos necessários para montar a trilha neste conjunto de etapas são: descrição de marca e modelo de componentes que podem ser utilizados na fabricação do HSM; e a existência de uma função que possibilite a inicialização segura do HSM.

6.3.1 FIPS 140-2

A seção 4.1 da norma FIPS 140-2 é dedicada a especificação do módulo criptográfico. Essa seção requer que seja indicado quais são os componentes de hardware do HSM, entre outras informações de especificação.

A norma não especifica qual é a profundidade das informações que são necessárias para descrever os componentes de hardware do HSM. É possível, num procedimento de homologação que os fabricantes tenham que indicar qual é a marca e modelo dos componentes utilizados a pedido da entidade homologadora. Entretanto a norma deixa a descrição aberta para diferentes interpretações. Portanto, pode ser que essas informações não sejam requeridas.

Para que o fabricante do HSM não fique dependente de determinados componentes, requer-se que todos os componentes e seus possíveis substitutos sejam especificados.

Para a etapa de transporte é necessário que os HSMs possuam uma funcionalidade nova para validar o HSM, detectando a substituição completa de um HSM ou tentativa de violação. Neste trabalho apresentamos a funcionalidade que utiliza uma chave de inicialização para resolver esse problema.

No capítulo 5 foi proposta a unificação das etapas do ciclo de vida do HSM com auditoria. Na seção 5.2.2, foi proposto o uso de uma chave de inicialização do HSM. Tal chave é gerada em fábrica e pode ser utilizada para inicializar um HSM após a sua chegada ao destino. A norma FIPS 140-2 deve incluir em sua descrição que um HSM deve dar suporte a esta funcionalidade.

A seção 4.10.2 da FIPS 140-2 indica quais são os requisitos de segurança para entrega, instalação e inicialização de um módulo criptográfico. Estes requisitos de segurança não deixam explícito o que é a entrega, instalação e inicialização segura.

Para estar de acordo com a proposta deste trabalho, a seção 4.10.2 deve deixar explícito que a segurança dos procedimentos de entrega, instalação e inicialização do HSM são baseados em proteções criptográficas, como a utilização de uma chave de inicialização que é gerada na montagem do HSM, e que garante a entrega segura.

A verificação de lacres de evidenciação de abertura e verificação da integridade do HSM são ações executadas pelo proprietário do HSM na inicialização do dispositivo, o que garante a instalação segura.

A seção 4.10.4 da FIPS 140-2 trata dos manuais e guias do administrador e usuário do HSM. A norma deve requerer na seção 4.10.4 que o manual do administrador contenha recomendações para garantir a integridade do dispositivo ao inicializá-lo.

O conjunto de alterações aqui proposto deve fazer parte do NSA da FIPS 140-2. As alterações nas seções 4.1, 4.10.2 e 4.10.4 reduzem a probabilidade de um HSM homologado possuir componentes maliciosos. Outra vantagem é a existência da inicialização segura baseada em

algoritmos criptográficos.

6.3.2 MCT 7

O MCT 7 é similar à FIPS 140-2 com relação aos requisitos relacionados a fabricação e transporte de HSMs.

O Requisito III.1.1 do MCT 7 também tem como requisito que os componentes de hardware do HSM sejam descritos, mas de forma superficial. O Requisito III.1.1 deve requerer que o fabricante indique qual são as marcas e modelos de componentes que serão utilizados na montagem do HSM.

O Requisito III.10.2 da norma MCT 7 requer que o fabricante deve listar os procedimentos específicos de instalação e inicialização segura do HSM. O MCT 7 também não indica o que é a instalação e inicialização segura, portanto o requisito pode ser interpretado de formas diferentes.

O Requisito III.10.2 deve ser modificado para especificar o que é a instalação e inicialização segura do HSM. De acordo com a proposta deste trabalho, a norma deve requerer que o fabricante implemente uma solução baseada em criptografia, como a chave de inicialização gerada durante a fabricação do HSM.

O Requisito III.10.4 da norma MCT 7 contém requisitos da documentação do administrador do HSM, que é o responsável por manter a segurança do módulo. Um item deve ser adicionado a esse requisito, requerendo que o "Guia do Administrador" descreva os procedimentos seguros para inicialização do HSM, como a verificação dos lacres de evidenciação de abertura e integridade do HSM.

Os requisitos modificados devem fazer parte do NSA do MCT 7.

6.4 GERENCIAMENTO DO HSM

O gerenciamento do HSM é um agrupamento de algumas das etapas do ciclo de vida do HSM. O gerenciamento do HSM é o conjunto das etapas de instalação, geração de chaves, utilização de chaves, auditorias periódicas e descarte.

A trilha de auditoria para as etapas do gerenciamento do HSM é gerada da mesma forma em todas essas etapas, com a geração detalhada de logs das operações executadas no HSM e posterior conferência com o log da cerimônia e políticas do proprietário do HSM.

6.4.1 FIPS 140-2

A seção 4.6.1 da norma FIPS 140-2 trata da gravação de logs de um HSM. Essa seção possui vários requisitos relacionados a gravação de logs quando funções específicas são executadas. Por exemplo, a adição ou remoção de um membro do grupo de administradores (crypto officer) deve ser gravada em log.

A seção 4.6.1 também requisita que o sistema operacional que detém o controle de software, firmware, chaves e qualquer informação de status, seja um sistema operacional com certificação *Common Criteria*. A *Common Criteria* é uma norma de homologação onde é possível depositar regras específicas de homologação, que são chamados de *Protection Profiles*. O sistema operacional do HSM deve possuir uma certificação *Common Criteria* com um *Protection Profile* definido pela FIPS 140-2.

O *Protection Profile* aceito pela FIPS 140-2 é constituído de várias regras que incluem a gravação de logs de auditoria. Porém, o conjunto de operações que devem ser gravadas em log permanece pequeno se comparado com o número de operações do HSM.

A proposta deste trabalho é que todas as operações executadas no HSM sejam gravadas em log, e não um conjunto de funções do HSM.

A seção 4.6.1 deve requerer que todas as operações executadas no HSM sejam gravadas em log, pois o log de operações é o artefato gerado pelo HSM para criar a trilha de auditoria das etapas do gerenciamento do HSM. A necessidade de gerar logs é um requisito que deve ser adicionado ao NSA da FIPS 140-2.

6.4.2 MCT 7

A seção 3.6 do MCT 7 que trata do ambiente operacional do HSM possui três requisitos e uma recomendação que indicam a necessidade da gravação de logs no HSM.

Os Requisitos III.6.3 e III.6.4 estão relacionados à homologação do sistema operacional e do ambiente operacional do HSM, respectivamente. Se o sistema operacional e o ambiente operacional já tem homologação por outra norma como a FIPS 140-2 e a *Common Criteria*, a documentação que comprova esta homologação pode ser depositada e irá facilitar o processo de homologação.

Se o uso do ambiente operacional foi homologado, isso significa que o HSM gera o log de algumas operações. Porém, conforme descrito

na seção 6.4.1, as normas FIPS 140-2 e a *Common Criteria* com o *Protection Profile* recomendado pela FIPS 140-2, requisitam que apenas um subconjunto das possíveis operações sejam gravadas em log.

Outros dois itens do MCT 7 requisitam que a execução de algumas operações sejam gravadas em log. No Requisito III.6.7 e na Recomendação III.6.1. A soma dos quatro requisitos citados nesta seção, não representam todas as operações executadas nas cerimônias de gerenciamento do HSM. Portanto, os requisitos para gravação de logs presentes na norma MCT 7 não são suficientes para permitir a auditoria das etapas de gerenciamento do HSM.

Um requisito deve ser adicionado ao MCT 7 requisitando que os logs de todas as operações executadas no HSM sejam gravados. Este requisito deve fazer parte do NSA do MCT 7.

6.5 DESCARTE

O descarte de um HSM significa que o ciclo de vida daquele HSM chegou ao fim, ou seja, ele não irá gerenciar as chaves criptográficas que manteve até então e não deve manter estas chaves armazenadas.

A trilha de auditoria da etapa de descarte é formada por apenas um artefato, o log de operações executadas. Ao contrário das etapas do gerenciamento do HSM, apenas o log de operações não é suficiente. É necessário que exista um mecanismo de limpeza do HSM para as ocasiões onde ele poderá ser re-utilizado.

A geração do log de operações já foi tratada na seção 6.4, onde os requisitos indicam que todas as operações devem ser gravadas em log. Portanto as operações de descarte também farão parte dos logs.

Esta seção comenta a questão da existência de uma função de limpeza do HSM, com a exportação do log de operações.

6.5.1 FIPS 140-2

A norma FIPS 140-2 não possui nenhum requisito relacionado ao descarte de um HSM. A única referência existente que é relacionada à remoção de conteúdo do HSM é o processo de "zeramento" de dados sensíveis.

O "zeramento" de dados contidos no HSM ocorre quando o conteúdo sensível (chaves, dados de autenticação, ...) não é mais necessário para as operações do HSM, e portanto a sua existência na memória deve

ser sobrescrita com zeros. Também é possível sobrescrever o conteúdo sensível com bits aleatórios.

Neste trabalho o procedimento de "zeramento" de conteúdo da memória não é considerado suficiente para o descarte do HSM. A proposta é que os dados contidos na memória volátil (memória RAM) e memória persistente (disco) do HSM sejam sobrescritos.

É necessário que os HSMs possuam uma função de descarte do dispositivo, para que a sobrescrita de dados da memória e disco de um HSM seja possível de ser executada. Esta função deve exportar o log de operações do HSM, para que os auditores possam comprovar que a limpeza do HSM foi executada.

O requisito que trata da função de limpeza do HSM poderia ser inserido na seção 4.6 ou na seção 4.7 da FIPS 140-2. A seção 4.6 trata de questões do ambiente operacional do HSM e a seção 4.7 trata do gerenciamento de chaves criptográficas. Este requisito deve fazer parte do NSA da FIPS 140-2.

6.5.2 MCT 7

Assim como ocorre na norma FIPS 140-2, o MCT 7 só possui requisitos relacionados ao "zeramento" de conteúdo sensível do HSM. O "zeramento" de conteúdo sensível contido na memória volátil não é suficiente para o descarte seguro do HSM.

Um requisito que descreve a necessidade de implementação da função de limpeza de dados do HSM, função descrita na seção 6.5.1, deve ser adicionado. Este requisito pode ser adicionado na seção 3.6 que trata de questões do ambiente operacional do HSM, ou na seção 3.7 que trata do gerenciamento de chaves do HSM. Este requisito deve fazer parte do NSA do MCT 7.

6.6 CONCLUSÃO

A contribuição deste capítulo é o complemento da proposta de unificação da auditoria no ciclo de vida de HSMs. O capítulo apresenta quais requisitos devem ser adicionados nas normas de homologação FIPS 140-2 e MCT 7 para possibilitar a auditoria unificada.

Por mais que exista uma definição teórica do que é um HSM, na prática os HSMs são implementados para atender aos requisitos das normas de homologação. A prática de mercado é implementar um HSM

que o cliente esteja interessado em comprar. Um cliente costuma adquirir HSMs que atendem as normas de homologação, pois eles confiam nessas normas. Portanto, os fabricantes tendem a comercializar HSMs que atendem as normas.

A proposta de inclusão e/ou alteração dos requisitos leva em consideração a compatibilidade com as normas já existentes, para facilitar o processo de transição entre as normas atuais, e as normas atualizadas com as alterações propostas.

Uma das normas que foram focadas nesse capítulo é a FIPS 140-2, pois é uma das normas mais conhecida e seguidas no mundo. A norma MCT 7 também faz parte das normas que ganharam foco neste trabalho pois é uma norma brasileira e que possui importância nacional. A norma MCT 7 foi criada com base na FIPS 140-2, e isso facilitou o processo de comparação e alteração dos requisitos realizados neste trabalho.

7 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Neste trabalho se buscou unificar a auditoria em HSMs. Para atingir este objetivo foi necessário mapear usuários e etapas do ciclo de vida de HSMs.

O capítulo 2 apresentou o ciclo de vida de chaves criptográficas. O entendimento desse ciclo de vida é necessário para o entendimento dos papéis de usuário e ciclo de vida de HSMs, que são apresentados no capítulo seguinte.

O capítulo 3 apresentou os tipos de papéis de usuário necessários para a gerência de chaves criptográficas. Usuários de HSMs possuem um número limitado de funções que podem executar em um dispositivo, portanto este capítulo descreveu quais são esses papéis de usuário e quais tipos de funções podem ser executados por cada papel de usuário. Esse capítulo também apresentou as etapas do ciclo de vida de um HSM e explicou brevemente que tipos de ações são executadas em cada etapa.

Ainda no capítulo 3 apresentou-se a definição de papéis de usuário das normas de homologação de HSMs, e a definição de (MARTINA; SOUZA; CUSTODIO, 2007). Nesse capítulo é realizada uma comparação entre as duas definições.

O capítulo 4 descreve com detalhes a leitura do ciclo de vida de HSMs que foi realizada neste trabalho. Para cada etapa do ciclo de vida de um HSM foi descrito um tipo de ataque. Para cada etapa foi descrito qual é a duração da etapa em uma situação comum, o ganho do adversário em um ataque, os recursos necessários para se realizar o ataque, o tempo necessário para executar o ataque e qual são os rastros de auditoria que devem ser deixados na execução normal da etapa.

Com a descrição do ciclo de vida de HSMs no capítulo 4, foi possível descrever a unificação da auditoria de HSMs no capítulo 5. Esse capítulo aborda o objetivo principal deste trabalho, que é poder executar a auditoria de qualquer etapa do ciclo de vida de um HSM, desde que os rastros de auditoria sejam gerados em todas as etapas.

É necessário que os HSMs sejam capazes de executar certas funcionalidades para gerar os rastros de auditoria descritos no capítulo 5. Fabricantes de HSMs seguem as normas de homologação para que haja maior aceitação do mercado de seu produto, e para que os compradores de HSMs possuam garantia de interoperabilidade e segurança dos equipamentos. Portando o capítulo 6 inclui nas normas de homologação as funcionalidades que possibilitam a geração de rastros de auditoria.

Com isso foi possível descrever a auditoria unificada em HSMs e encontrar uma forma de adicionar estes requisitos nas normas de homologação, buscando sempre diminuir o impacto aos processo de homologação e fabricação de HSMs que já existem.

Com este trabalho é possível verificar que existe espaço para o aprimoramento das normas de homologação de HSMs. As normas podem ser aprimoradas no que diz respeito ao controle das interações com o dispositivo, por exemplo a interação com smartcards.

As normas FIPS 140-2 e MCT 7 não requerem que a autenticação por prova de posse (smartcard e token) nos HSMs, seja realizada com dispositivos homologados. É possível utilizar smartcards com nível de proteção baixo em HSMs homologados. Caso sejam utilizados smartcards maliciosos em um HSM, é possível burlar a prova de posse na autenticação de usuários e utilizar as chaves gerenciadas.

Também é possível notar que as normas de homologação delegam a verificação dos sistemas operacionais para outros órgãos e outras normas de homologação. As normas de homologação de HSMs focam bastante na proteção de chaves no disco rígido, autenticação, proteção física do dispositivo, mitigação de ataques e proteção do software de gerência do HSM, porém não possuem requisitos de proteção do sistema operacional.

As normas FIPS 140-2 e MCT 7 requerem que o sistema operacional ou o ambiente operacional do HSM sejam homologados pela norma *Common Criteria*, com a utilização de perfis de proteção específicos. Uma proposta é que os órgãos homologadores de HSMs possuam formas de realizar testes de segurança no sistema operacional do HSM.

REFERÊNCIAS

CARLOS, M.; CUSTODIO, R.; SUTIL, J. Good practices for long-term key management in a public key infrastructure. In: *Computational Science and Engineering Workshops, 2008. CSEWORKSHOPS '08. 11th IEEE International Conference on.* [S.l.: s.n.], 2008. p. 141 –148.

GALLO, R.; KAWAKAMI, H.; DAHAB, R. On device identity establishment and verification. In: *Proceedings of the 6th European conference on Public key infrastructures, services and applications.* Berlin, Heidelberg: Springer-Verlag, 2010. (EuroPKI'09), p. 130–145. ISBN 3-642-16440-4, 978-3-642-16440-8. Disponível em: <http://dl.acm.org/citation.cfm?id=1927830.1927843>.

GALLO, R.; KAWAKAMI, H.; DAHAB, R. Fortuna - a probabilistic framework for early design stages of hardware-based secure systems. In: *Network and System Security (NSS), 2011 5th International Conference on.* [S.l.: s.n.], 2011. p. 184 –191.

MARTINA, J.; SOUZA, T. de; CUSTODIO, R. Openhsm: An open key life cycle protocol for public key infrastructure's hardware security modules. In: LOPEZ, J.; SAMARATI, P.; FERRER, J. (Ed.). *Public Key Infrastructure.* Springer Berlin / Heidelberg, 2007, (Lecture Notes in Computer Science, v. 4582). p. 220–235. ISBN 978-3-540-73407-9. 10.1007/978-3-540-73408-6_16. Disponível em: <http://dx.doi.org/10.1007/978-3-540-73408-6_16>.

MARTINA, J.; SOUZA, T. Salavaro de; CUSTODIO, R. Ceremonies formal analysis in pki's context. In: *Computational Science and Engineering, 2009. CSE '09. International Conference on.* [S.l.: s.n.], 2009. v. 3, p. 392 –398.

MENEZES, A. J. et al. *Handbook of Applied Cryptography.* 1997.

NIST. *FIPS PUB 140-2, Security Requirements for Cryptographic Modules.* maio 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

SOUZA, T. C. S. de; MARTINA, J. E.; CUSTóDIO, R. F. Audit and backup procedures for hardware security modules. In: *Proceedings of the 7th symposium on Identity and trust on the Internet.* New York,

NY, USA: ACM, 2008. (IDtrust '08), p. 89–97. ISBN 978-1-60558-066-1. Disponível em: <http://doi.acm.org/10.1145/1373290.1373302>.

TEHRANIPOOR, M.; KOUSHANFAR, F. A survey of hardware trojan taxonomy and detection. *Design Test of Computers, IEEE*, v. 27, n. 1, p. 10 –25, jan.-feb. 2010. ISSN 0740-7475.

YOUNG, A.; YUNG, M. Kleptography: Using cryptography against cryptography. In: FUMY, W. (Ed.). *Advances in Cryptology – EUROCRYPT '97*. Springer Berlin Heidelberg, 1997, (Lecture Notes in Computer Science, v. 1233). p. 62–74. ISBN 978-3-540-62975-7. Disponível em: <http://dx.doi.org/10.1007/3-540-69053-0_6>.